

Sample security assessment: acme.example

Kestrel Freight

Part I: Executive

Executive summary, remediation roadmap, ATT&CK snapshot, compliance snapshot

Part II: Technical

Scope, methodology, findings, attack surface, narrative, vulnerability intelligence, compliance, history

Target	acme.example (Domain)
Profile	Deep
Assessment finished	26 Sep 2026 17:56 UTC
Prepared for	Kestrel Freight
Prepared by	Sam Rivera, Lead Security Consultant (fictional), AQIRA sample
Prepared on	29 September 2026
Issue	v1
Classification	Confidential

Document control

Properties

Document id	scn_cb416011e91841c3-v1
Issue	v1 (professional)
Template	Executive Cyber
Generated	29 Sep 2026 09:30 UTC
Classification	Confidential
Prepared by	Sam Rivera, Lead Security Consultant (fictional)
Reviewed by	not recorded
Approved by	(signature)
Distribution	Kestrel Freight; AQIRA sample

Version history

Issue	Kind	Template	Created	Status	Formats
v1	professional	Executive Cyber	29 Sep 2026 09:30 UTC	this issue	html (included), json (included), md (included)

Integrity

Format	Content type	SHA-256	Bytes
html	text/html; charset=utf-8	see the report library (hashes of this document cannot be embedded in itself)	n/a
json	application/json; charset=utf-8	see the report library (hashes of this document cannot be embedded in itself)	n/a
md	text/markdown; charset=utf-8	see the report library (hashes of this document cannot be embedded in itself)	n/a

Operator identities are redacted from this issue (history and governance entries record that an operator acted, not who).

Confidentiality, disclaimer and authorisation

This document is classified **Confidential** and is intended for Kestrel Freight. It describes the security posture of acme.example as observed by an automated assessment at a single point in time (26 Sep 2026 17:56 UTC); conditions may have changed since. The run was executed under the authorisation recorded at the time it was started.

Handling

Distribute only to the named recipients. Store encrypted at rest, do not forward outside the organisation without the reporter's consent, and destroy superseded issues when a newer one is accepted. Evidence in this report is illustrative and benign: probes carry plain-text markers and read-only requests, never working exploits.

Authorisation and scope

Profile **Deep** with the phases Reconnaissance, Web and API Security, Infrastructure and Configuration, Exploitability Validation, Review and Reporting. Active testing was authorised by the requesting account. Targets are limited to acme.example and the assets discovered from it; internal ranges are covered only where a collector is enrolled (Appendix A).

Disclaimer

Findings reflect what the assessment engine could observe with its capabilities on the date of the run. Absence of a finding is not proof of absence of a weakness. Severity is engine-assigned; CVSS scores are informative. Risk scores follow the formula in the methodology section and are not recomputed after triage.

Data provenance

Every figure in this issue is drawn from the assessment platform's records for this run and account. Console modules that are demonstration fixtures are excluded from every report (cloud, microsoft, code-security, mobile-package, threat-intel-kev, threat-intel-exposure, threat-intel-iocs, threat-intel-actors, threat-geography, compliance-stub-frameworks); see Appendix E.

Contents

Document control	
Confidentiality, disclaimer and authorisation	
1 Executive summary	
2 Remediation roadmap	
3 MITRE ATT&CK coverage	
4 Compliance and control mapping	
5 Scope, objectives and rules of engagement	
6 Methodology and rating method	
7 Findings summary	
8 Detailed findings	
F-01 Backdoored xz/liblzma package installed	F-08 Database port reachable from the internet
F-02 SQL injection in search parameter	F-09 Outdated TLS protocol versions accepted
F-03 Apache HTTP Server path traversal	F-10 Login portal does not enforce multi-factor authentication
F-04 Default credentials accepted on management service	F-11 Security headers missing (CSP, HSTS)
F-05 Source control metadata exposed (.git directory)	F-12 Directory listing enabled
F-06 Dangling DNS record allows subdomain takeover	9 Attack surface and asset inventory
F-07 Publicly listable cloud storage bucket	10 Attack narrative and kill chain
	11 Vulnerability intelligence
	12 Compliance and control mapping
	13 Assessment history and trend
	14 Conclusion and next steps
	Appendix A: Agents, capabilities and datasets
	Appendix B: Severity, risk and CVSS definitions
	Appendix C: Glossary
	Appendix D: Evidence index and activity log
	Appendix E: Report metadata and provenance

Figures

Figure 1: Risk score 100 of 100 (Critical); open-only score 100.

Figure 2: Findings by severity: outer ring observed in this run, inner ring still open.

Figure 3: Status of the run's findings.

Figure 4: Change against the previous run.

Figure 5: Actionable items by tier and effort.

Figure 6: The five techniques with the most findings.

Figure 7: Share of findings mapped per framework, with the groups reached.

Figure 8: Implemented share of applicable controls (tenant-wide governance state).

Figure 9: Phase timeline of the run.

Figure 10: The assessment pipeline.

Figure 11: Findings by severity and status.

Figure 12: CVSS vector
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H.

Figure 13: CVSS vector
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H.

Figure 14: CVSS vector
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N.

Figure 15: CVSS vector
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H.

Figure 16: CVSS vector
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N.

Figure 17: CVSS vector
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:H/A:N.

Figure 18: CVSS vector
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N.

Figure 19: CVSS vector
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:L.

Figure 20: CVSS vector
CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N.

Figure 21: CVSS vector
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N.

Figure 22: CVSS vector
CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N.

Figure 23: CVSS vector
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N.

Figure 24: Topology: external lane above, internal below; dashed links cross the boundary, node colour is the worst finding severity.

Figure 25: Assets by kind.

Figure 26: Assets by exposure.

Figure 27: Activity across the run: findings, discoveries and activity lines per phase.

Figure 28: Tactic sequence of admin.acme.example to admin.acme.example.

Figure 29: Tactic sequence of https/443 tomcat to https/443 tomcat.

Figure 30: Findings raised in each phase by severity.

Figure 31: CVEs by number of findings referencing them (top 8).

Figure 32: CVSS base scores of the referenced CVEs.

Figure 33: Share of findings mapped per framework, with the groups reached.

Figure 34: Implemented share of applicable controls (tenant-wide governance state).

Figure 35: OWASP Top 10 2021: control status across 10 applicable controls.

Figure 36: NIST CSF 2.0: control status across 104 applicable controls.

Figure 37: NIST SP 800-53 Rev 5: control status across 182 applicable controls.

Figure 38: NIST SP 800-171 Rev 2: control status across 104 applicable controls.

Figure 39: COBIT 2019: control status across 40 applicable controls.

Figure 40: Risk score across completed runs.

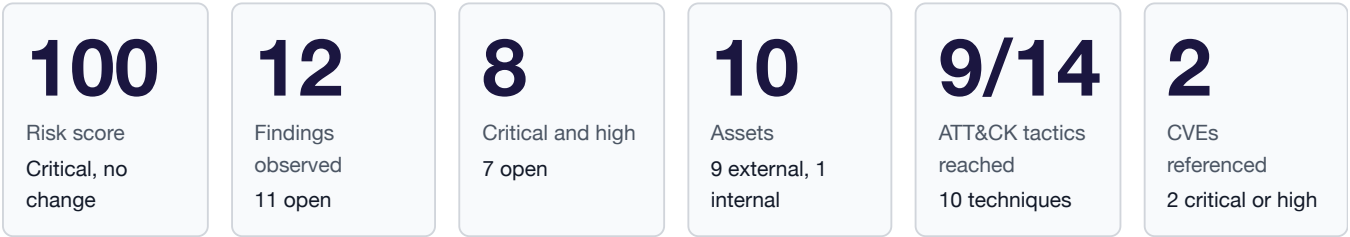
Figure 41: Findings per run by severity.

Figure 42: Share of declared capabilities each agent exercised in this run.

Part I: Executive

What the leadership team needs: the posture, the top risks, the plan and the coverage snapshots.

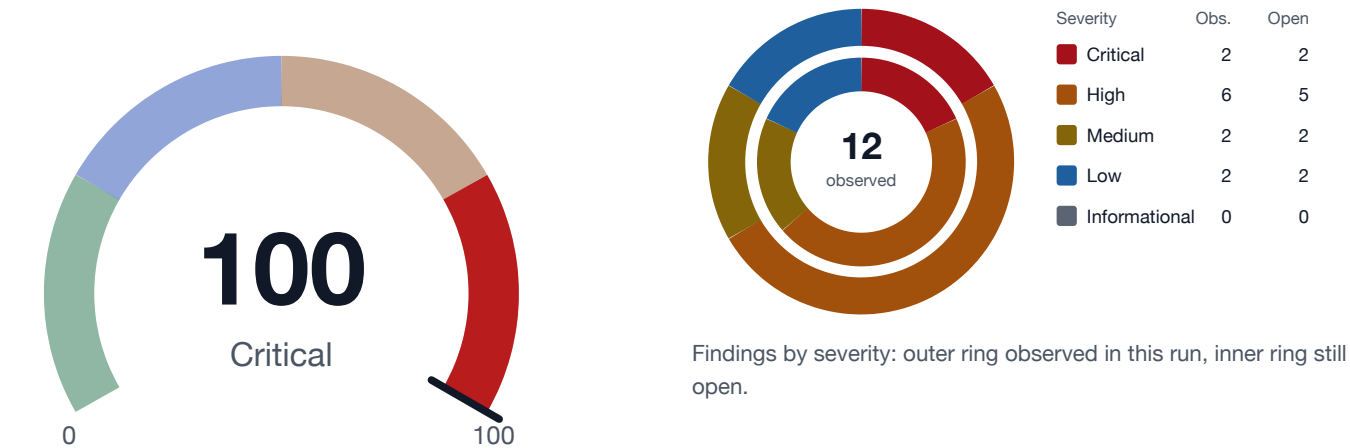
1. Executive summary



The deep assessment of acme.example completed on 26 September 2026 with a risk score of 100 (Critical), unchanged from the previous run. 12 findings were observed across 10 assets: 2 critical, 6 high, 2 medium, 2 low. By status: 11 open, 1 marked as a false positive.

The most significant open exposures are Backdoored xz/liblzma package installed on admin.acme.example (F-01, critical, externally reachable); SQL injection in search parameter on https/443 tomcat (F-02, critical, externally reachable); and Dangling DNS record allows subdomain takeover on status.acme.example (F-06, high, externally reachable). 2 derived attack paths link externally reachable assets to onward targets.

Compared with the previous run, 0 findings are new, 0 were resolved and 12 persist. 6 items fall in the immediate remediation tier and 1 in the short-term tier; 3 are quick wins.



Risk score 100 of 100 (Critical); open-only score 100.



Top open risks

Ref	Finding	Severity	Asset	Business impact
F-01	Backdoored xz/liblzma package installed	Critical	admin.acme.example	Pre-authentication compromise of sshd.
F-02	SQL injection in search parameter	Critical	https/443 tomcat	Read and modify the application database.

Ref	Finding	Severity	Asset	Business impact
F-06	Dangling DNS record allows subdomain takeover	High	status.acme.example	Phishing and cookie theft from a trusted subdomain.
F-08	Database port reachable from the internet	High	admin.acme.example	Direct brute force and exploitation of the database.
F-03	Apache HTTP Server path traversal	High	https/443 tomcat	Disclosure of configuration files and, with CGI enabled, remote code execution.

Remediation tiers

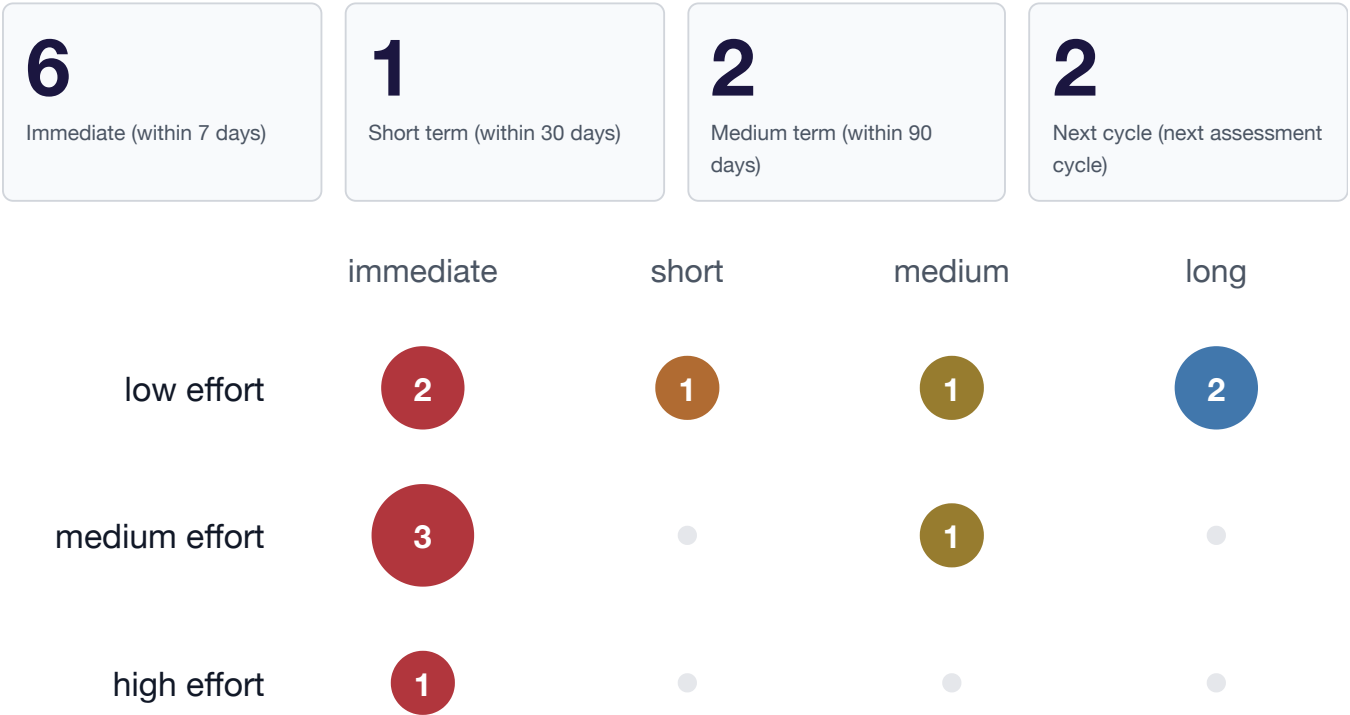
Immediate: 6

Short term: 1

Medium term: 2

Next cycle: 2

2. Remediation roadmap



Actionable items by tier and effort.

Remediation tiers

Tier	Window	Criteria	Items	Refs
Immediate	within 7 days	critical; or high with KEV listing or EPSS at or above 0.10; or high with high confidence on an external asset	6	F-01 F-02 F-08 F-03 F-05 F-07
Short term	within 30 days	remaining high	1	F-06
Medium term	within 90 days	medium	2	F-10 F-09
Next cycle	next assessment cycle	low and informational	2	F-12 F-11

Quick wins

- F-05 Source control metadata exposed (.git directory) (Remove .git from the deployed artefact and deny dot-paths at the web server.)
- F-07 Publicly listable cloud storage bucket (Block public access on the bucket and serve assets through a CDN origin access identity.)
- F-06 Dangling DNS record allows subdomain takeover (Delete the stale record or reclaim the target resource.)

Decisions needed

- Assign owners and target dates to the 6 immediate items (the POA&M table leaves both blank on purpose).
- Fund the 4 programme themes below rather than fixing findings one by one.

- Confirm the retest cadence and who signs off closed findings.

Strategic themes

Security Misconfiguration

6 findings in this assessment fall under A05:2021 (Security Misconfiguration). Treat the category as a programme item: assign an owner, set a standard for new work and verify it on the next cycle rather than closing findings one by one.

owasp A05:2021; findings **F-05 F-06 F-07 F-08 F-11 F-12**

Broken Access Control

4 findings in this assessment fall under A01:2021 (Broken Access Control). Treat the category as a programme item: assign an owner, set a standard for new work and verify it on the next cycle rather than closing findings one by one.

owasp A01:2021; findings **F-03 F-05 F-07 F-12**

Vulnerable and Outdated Components

2 findings in this assessment fall under A06:2021 (Vulnerable and Outdated Components). Treat the category as a programme item: assign an owner, set a standard for new work and verify it on the next cycle rather than closing findings one by one.

owasp A06:2021; findings **F-01 F-03**

Cryptographic Failures

1 finding in this assessment fall under A02:2021 (Cryptographic Failures). Treat the category as a programme item: assign an owner, set a standard for new work and verify it on the next cycle rather than closing findings one by one.

owasp A02:2021; findings **F-09**

Plan of action and milestones

Ref	Title	Severity	Tier	Rank	Effort	Status	Owner	Target date	Verification
F-01	Backdoored xz/liblzma package installed	Critical	Immediate	1	High	Open	_____	_____	retest
F-02	SQL injection in search parameter	Critical	Immediate	2	Medium	Open	_____	_____	retest
F-08	Database port reachable from the internet	High	Immediate	3	Medium	Open	_____	_____	retest
F-03	Apache HTTP Server path traversal	High	Immediate	4	Medium	Open	_____	_____	retest
F-05	Source control metadata exposed (.git directory)	High	Immediate	5	Low	Open	_____	_____	retest
F-07	Publicly listable cloud storage bucket	High	Immediate	6	Low	Open	_____	_____	retest
F-06	Dangling DNS record allows subdomain takeover	High	Short term	1	Low	Open	_____	_____	retest

Ref	Title	Severity	Tier	Rank	Effort	Status	Owner	Target date	Verification
F-10	Login portal does not enforce multi-factor authentication	Medium	Medium term	1	Medium	Open			rescan
F-09	Outdated TLS protocol versions accepted	Medium	Medium term	2	Low	Open			rescan
F-12	Directory listing enabled	Low	Next cycle	1	Low	Open			rescan
F-11	Security headers missing (CSP, HSTS)	Low	Next cycle	2	Low	Open			rescan

Retest

A retest is recommended once the immediate and short-term tiers are addressed; a weekly schedule exists for this target, next run 3 Oct 2026 17:03 UTC.

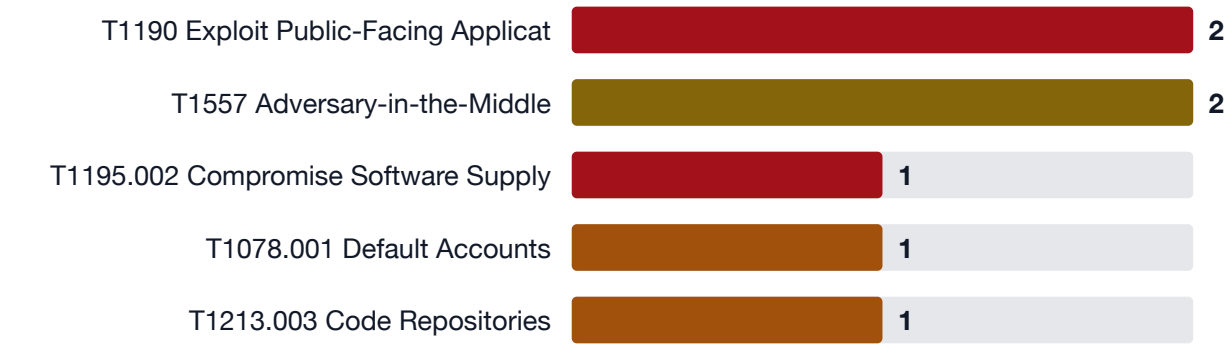
3. MITRE ATT&CK coverage

12/12 Findings mapped 0 unmapped	9/14 Tactics reached	10/202 Techniques covered sub-techniques count toward their parent	2 Derived attack paths
--	--	--	--

ATT&CK Enterprise v15.1: techniques with findings

Reconnaissance 1/38	Resource Development 2/35	Initial Access 5/21	Execution 0/29	Persistence 2/52	Privilege Escalation 2/35	Defense Evasion 2/86	Credential Access 3/59	Discovery 1/39	Lateral Movement 0/21	Collection 4/26	Command and Control 0/26	Exfiltration 0/16	Impact 0/25
T1594 Search Victim-Owned Websites (1)	T1584.001 Domains (1)	T1078.001 Default Accounts (1)		T1078.001 Default Accounts (1)	T1078.001 Default Accounts (1)	T1078.001 Default Accounts (1)	T1110.004 Credential Stuffing (1)	T1046 Network Service Discovery (1)		T1213.003 Code Repositories (1)			
		T1190 Exploit Public- Facing Application (2)					T1557 Adversary-in- the-Middle (2)			T1530 Data from Cloud Storage (1)			
		T1195.002 Compromise Software Supply Chain (1)								T1557 Adversary-in- the-Middle (2)			

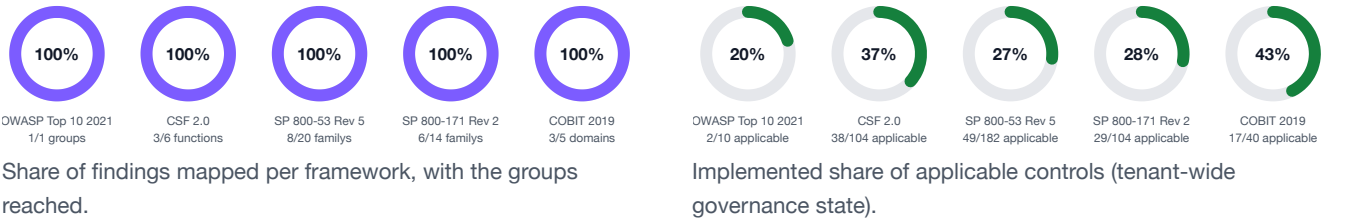
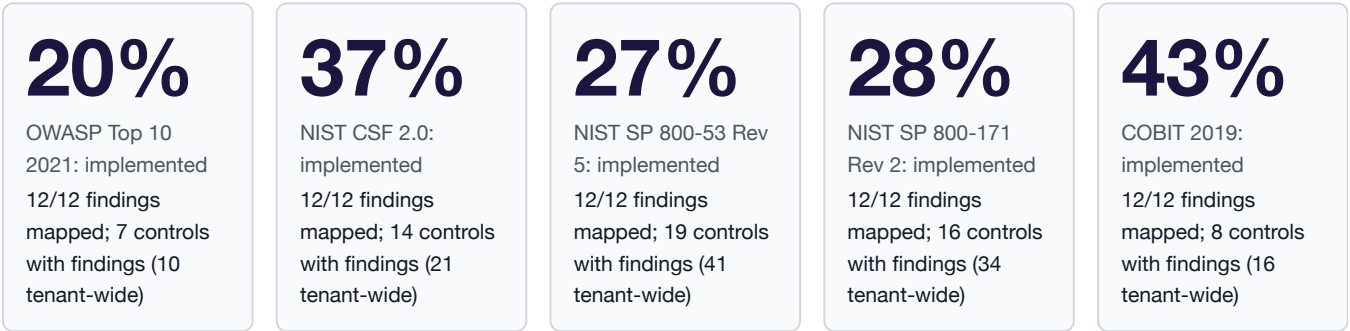
None findings 1 finding 2-3 findings 4-9 findings 10+ findings



The five techniques with the most findings.

The full matrix and technique table are in Part II.

4. Compliance and control mapping



Control status, owner, note and evidence are tenant-wide governance state shared by every assessment of the account, snapshotted when this issue was generated; only the mapped-findings figures are scoped to this assessment. 'Controls with findings' is given both for this run and tenant-wide, the latter being the number the console's compliance band prints.

Control tables and the crosswalk are in Part II.

Part II: Technical

What engineering needs: scope, method, every finding with evidence, the attack surface, the narrative and the full coverage tables.

5. Scope, objectives and rules of engagement

Sample report published on the AQIRA website. Kestrel Freight is a fictional client and acme.example is a reserved example domain; every finding comes from AQIRA demo data.

Scope

Item	Value
Scope of work	Sample report published on the AQIRA website. Kestrel Freight is a fictional client and acme.example is a reserved example domain; every finding comes from AQIRA demo data.
Target	acme.example (Domain)
Profile	Deep
Phases	Reconnaissance, Web and API Security, Infrastructure and Configuration, Exploitability Validation, Review and Reporting
Authorised active testing	Yes
Started / finished	26 Sep 2026 17:12 UTC / 26 Sep 2026 17:56 UTC (44 min)
Internal coverage	Legacy VPN probe (revoked, authorised; 10.99.0.0/16); Frankfurt data centre sensor (active, authorised; 10.20.0.0/16, 172.16.8.0/22); Amsterdam office sensor (active, authorised; 10.10.0.0/16); Singapore office sensor (pending; 192.168.40.0/24); Contoso DC collector (active, authorised; ad:forest:corp.example.com)

Objectives

- Map the externally reachable attack surface of the target and the assets linked to it.
- Identify weaknesses on those assets, rate their severity and confirm exploitability with benign probes where the profile allows.
- Place each finding on the MITRE ATT&CK matrix and map it to the tracked compliance frameworks.
- Provide a prioritised, verifiable remediation plan and a baseline for the next run.

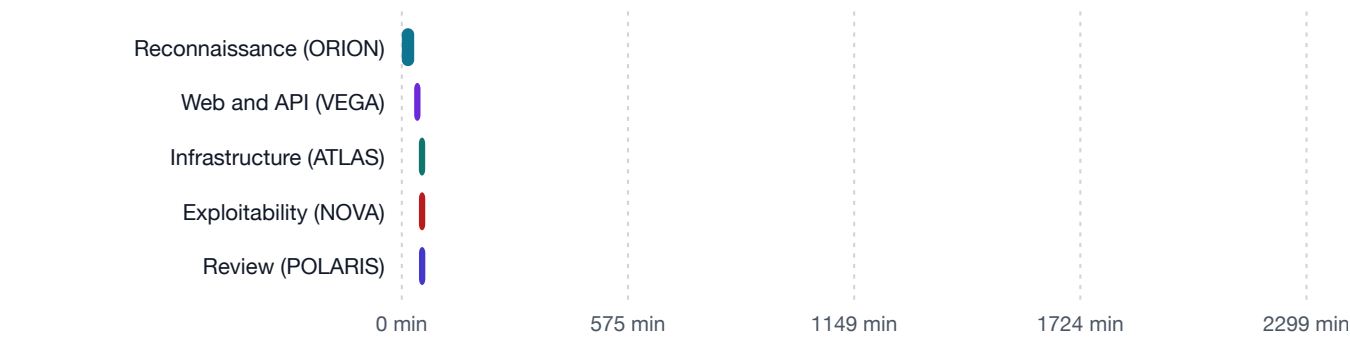
Rules of engagement

Active probes were limited to benign, marker-carrying and read-only requests; no state-changing request, credential use or denial-of-service test was performed. Internal ranges are only assessed through an enrolled collector with explicit authorisation.

Limitations

- Console modules that are demonstration fixtures are excluded (10 modules, Appendix E).

Timeline



Phase	Agent	State	Started	Ended	Duration	Findings	Discoveries
Reconnaissance	ORION	done	26 Sep 2026 17:12 UTC	26 Sep 2026 17:44 UTC	31 min	2	5
Web and API Security	VEGA	done	26 Sep 2026 17:44 UTC	26 Sep 2026 17:56 UTC	12 min	6	2
Infrastructure and Configuration	ATLAS	done	26 Sep 2026 17:56 UTC	26 Sep 2026 17:56 UTC	11 s	2	3
Exploitability Validation	NOVA	done	26 Sep 2026 17:56 UTC	26 Sep 2026 17:56 UTC	11 s	2	0
Review and Reporting	POLARIS	done	26 Sep 2026 17:56 UTC	26 Sep 2026 17:56 UTC	9 s	0	0

Team

- Reporter

Sam Rivera, Lead Security Consultant (fictional)
- Reviewer

not recorded
- Organisation

AQIRA sample
- Agents

ORION (Maps the public attack surface); VEGA (Probes web and API input handling, sessions, and headers); ATLAS (Assesses cloud, transport, and the internal segment); NOVA (Validates exploitability to benign proof); POLARIS (Consolidates findings and maps them to control frameworks); SCRIBE (Writes the client-deliverable report)

6. Methodology and rating method

The assessment runs a fixed pipeline of five phases, each owned by an autonomous agent with a declared set of capabilities. The phases below are those of a Deep run; greyed phases are not part of this profile.



The assessment pipeline.

Phase	Agent	Capabilities	In this run
Reconnaissance	ORION	Open-source intel, DNS intelligence, Vulnerability correlation, Source-code review	Yes
Web and API Security	VEGA	Source-code review, Dependency risk, Integration scanning	Yes
Infrastructure and Configuration	ATLAS	Cloud posture, DNS intelligence, Dependency risk, Vulnerability correlation	Yes
Exploitability Validation	NOVA	Offensive toolchain, Vulnerability correlation, Browser attack paths, Breach exposure, Hidden-data inspection, Remote-asset exposure	Yes
Review and Reporting	POLARIS	synthesis only	Yes

Rating method

Severity is assigned per finding by the assessment engine's finding model from impact and exploitability; the CVSS v3.1 base score and vector are printed as informative context and do not override it.

Risk score = $\min(100, \text{critical} \times 25 + \text{high} \times 12 + \text{medium} \times 5 + \text{low} \times 2 + \text{info} \times 0)$ over every finding observed in the run, frozen when the run finished and not recomputed after triage. The open-only score applies the same formula to findings still open.

Risk bands

Band	Score range
Low	0 to 24
Moderate	25 to 49
Elevated	50 to 74
Critical	75 to 100

Severity model

Severity	CVSS band	Definition
Critical	9.0 to 10.0	Exploitable without preconditions, with a direct path to full compromise of the affected system or data.
High	7.0 to 8.9	Significant impact with realistic exploitation, or a weakness that materially shortens an attacker's path.

Severity	CVSS band	Definition
Medium	4.0 to 6.9	Moderate impact, or exploitation depends on preconditions such as user interaction or an existing foothold.
Low	0.1 to 3.9	Limited impact on its own; typically hardening or hygiene.
Informational	0.0	An observation without direct security impact, recorded for completeness.

Confidence

Confidence	Meaning
high	Confirmed by benign proof: a marker echo, a version readout or a configuration value observed directly.
medium	Consistent with the advisory or the observed behaviour, but exploitation depends on the deployment shape.
low	Inferred from indirect signals; verification is recommended before remediation is scheduled.

Finding status

Status	Meaning
Open	Reported and not yet addressed.
In remediation	A fix is in progress; the finding remains counted until a retest confirms it.
Accepted risk	The owner has accepted the risk, with a reason and, where set, an expiry date for the exception.
Resolved	Closed; a rescan or retest no longer observes the condition.
False positive	Reviewed and judged not to be a real weakness.

Evidence handling

Evidence is recorded per phase as structured key and value pairs: benign probes, observed responses, version readouts and configuration values. Probes carry a plain-text marker and never a working exploit. Secrets are masked before storage, and evidence the platform withholds for safety is marked as withheld rather than printed.

Standards referenced

- PTES Technical Guidelines (Reporting), <http://www.pentest-standard.org/index.php/Reporting>
- NIST SP 800-115 Technical Guide to Information Security Testing and Assessment (2008), <https://csrc.nist.gov/pubs/sp/800/115/final>
- MITRE ATT&CK Enterprise (v15.1), <https://attack.mitre.org/>
- CVSS v3.1 Specification (3.1), <https://www.first.org/cvss/v3.1/specification-document>

7. Findings summary

All findings observed in this run

Ref	Title	Severity	CVSS	Conf.	Status	Asset	Exposure	Technique	CVEs	Change	Tags
F-01	Backdoored xz/liblzma package installed	Critical	10.0	Low	Open	admin.acme.example	External	T1195.002 Compromise Software Supply Chain	CVE-2024-3094	Persisting	Internet facing Vendor patch required
F-02	SQL injection in search parameter	Critical	9.8	High	Open	https/443 tomcat	External	T1190 Exploit Public-Facing Application		Persisting	Internet facing PCI scope Quick win
F-03	Apache HTTP Server path traversal	High	7.5	High	Open	https/443 tomcat	External	T1190 Exploit Public-Facing Application	CVE-2021-41773	Persisting	Internet facing PCI scope Vendor patch required
F-04	Default credentials accepted on management service	High	8.8	High	False positive	https/443 tomcat	External	T1078.001 Default Accounts		Persisting	Internet facing PCI scope Vendor patch required
F-05	Source control metadata exposed (.git directory)	High	7.5	High	Open	admin.acme.example	External	T1213.003 Code Repositories		Persisting	Internet facing
F-06	Dangling DNS record allows subdomain takeover	High	8.2	Medium	Open	status.acme.example	External	T1584.001 Domains		Persisting	Internet facing
F-07	Publicly listable cloud storage bucket	High	7.5	High	Open	acme.example-assets	External	T1530 Data from Cloud Storage		Persisting	Internet facing Quick win

Ref	Title	Severity	CVSS	Conf.	Status	Asset	Exposure	Technique	CVEs	Change	Tags
F-08	Database port reachable from the internet	High	8.1	High	Open	admin.acme.example	External	T1046 Network Service Discovery		Persisting	Internet facing PCI scope
F-09	Outdated TLS protocol versions accepted	Medium	5.9	High	Open	https/443 tomcat	External	T1557 Adversary-in-the-Middle		Persisting	Needs owner PCI scope
F-10	Login portal does not enforce multi-factor authentication	Medium	6.5	Medium	Open	admin.acme.example	External	T1110.004 Credential Stuffing		Persisting	Needs owner
F-11	Security headers missing (CSP, HSTS)	Low	3.1	High	Open	admin.acme.example	External	T1557 Adversary-in-the-Middle		Persisting	Quick win
F-12	Directory listing enabled	Low	3.7	High	Open	admin.acme.example	External	T1594 Search Victim-Owned Websites		Persisting	Quick win

12 findings; 0 without a technique, 0 without a control mapping.

	Open	Accepted risk	In remediation	Resolved	False positive
Critical	2	0	0	0	0
High	5	0	0	0	1
Medium	2	0	0	0	0
Low	2	0	0	0	0
Informational	0	0	0	0	0

Findings by severity and status.

8. Detailed findings

12 findings in severity order. Each block gives the observation, its impact, the benign evidence, the remediation with its tier and effort, references and the lifecycle history.

F-01

Backdoored xz/liblzma package installed

Critical

Open

CVSS 10.0 Confidence Low External Persisting from the previous run First seen 5 Sep 2026 14:18 UTC
Last seen 26 Sep 2026 17:56 UTC AQ-000024

Affected asset: admin.acme.example (also observed in 2 other runs)
Locations: admin.acme.example:22

SUMMARY

The SSH banner and package fingerprint match a distribution build shipping xz 5.6.0/5.6.1.

The host db-01.internal reports a package fingerprint matching xz 5.6.1, a build associated with a supply-chain compromise of the compression library used by the SSH stack.

Root cause (third_party): A compromised upstream package version is present on the host.

BUSINESS IMPACT

Pre-authentication compromise of sshd.
A compromised compression library in the SSH path can undermine authentication on the host before a user signs in.

LIKELIHOOD AND EXPLOITABILITY

Confidence Low, likelihood possible; KEV listing not available. The match is by fingerprint and needs confirmation, so confidence is low and likelihood possible.

AV
N

AC
L

PR
N

UI
N

S
C

C
H

I
H

A
H

CVSS vector CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H.

EVIDENCE

Observed 26 Sep 2026 17:56 UTC in exploit

banner: SSH-2.0-OpenSSH_9.6p1 Debian-4
package: xz-utils 5.6.1-1

REPRODUCTION STEPS

Preconditions: Inventory or host access to admin.acme.example

1. Read the SSH banner

Expected: An OpenSSH banner on a distribution linking liblzma

2. Read the xz-utils package version

Expected: 5.6.0 or 5.6.1

PROOF OF CONCEPT (BENIGN)

Kind

service

Title

Package version readout

Request

Read the SSH banner and package inventory on admin.acme.example

Response

SSH-2.0-OpenSSH_9.6p1 Debian-4; xz-utils 5.6.1-1

Notes The banner and package version are read from inventory. No exploitation is attempted.

REMEDIATION

Downgrade xz-utils to 5.4.x and rebuild affected hosts from a clean image.

1. Pin xz-utils to a safe 5.4.x version (contain, low effort, P0)
2. Rebuild affected hosts from a clean, verified image (fix, high effort, P0)
3. Add SBOM and provenance checks to the build and deploy path (harden, high effort, P2)

Tier: Immediate (rank 1); effort High (template); fixed in xz-utils 5.4.6.

VERIFICATION

Retest status: not_retested

1. Re-read the package version
Expected: A safe 5.4.x version

ATT&CK MITIGATIONS

- M1016 Vulnerability Scanning: Continuous monitoring of vulnerability sources and the use of automatic and manual code review tools should also be implemented as well.
- M1051 Update Software: A patch management process should be implemented to check unused applications, unmaintained and/or previously vulnerable software, unnecessary features, components, files, and documentation.

ATT&CK DETECTION

- File / File Metadata: Use verification of distributed binaries through hash checking or other integrity checking mechanisms. Scan downloads for malicious signatures and attempt to test software and updates prior to deployment while taking note of potential suspicious activity.

DETECTION

- File / File Metadata: Package inventory reporting xz-utils 5.6.0 or 5.6.1.

ATT&CK

T1195.002 Compromise Software Supply Chain: Initial Access

CONTROLS

- **owasp** A08:2021 Software and Data Integrity Failures
- **owasp** A06:2021 Vulnerable and Outdated Components
- **nistcsf** ID.RA-09 The authenticity and integrity of hardware and software are assessed prior to acquisition and use
- **nistcsf** PR.PS-02 Software is maintained, replaced, and removed commensurate with risk
- **nist80053** SR-3 Supply Chain Controls and Processes
- **nist80053** SR-11 Component Authenticity
- **nist80053** SI-7 Software, Firmware, and Information Integrity
- **nist80053** SI-2 Flaw Remediation
- **nist800171** 3.14.1 Identify, report, and correct system flaws in a timely manner.
- **nist800171** 3.14.2 Provide protection from malicious code at designated locations within organizational systems.
- **cobit** APO10 Managed Vendors
- **cobit** APO12 Managed Risk

REFERENCES

- CVE-2024-3094
- CWE-506

- ATT&CK T1195.002 Compromise Software Supply Chain (Initial Access)
- CVE-2024-3094
- CWE-506
- ATT&CK T1195.002

Lifecycle

When	From	To	By	Note
5 Sep 2026 14:18 UTC	created	Open	engine	n/a
7 Sep 2026 14:18 UTC	Open	Accepted risk	operator	Risk accepted for 30 days while the vendor patch is validated in staging.
14 Sep 2026 14:15 UTC	Accepted risk	Open	operator	Reopened: the follow-up assessment observed the issue again.

Internet facing Vendor patch required

F-02 SQL injection in search parameter

Critical Open

CVSS 9.8 Confidence High External Persisting from the previous run First seen 27 Aug 2026 14:14 UTC
Last seen 26 Sep 2026 17:56 UTC AQ-000002

Affected asset: https/443 tomcat (also observed in 4 other runs)
Locations: https://api.acme.example/search

SUMMARY

The q parameter is concatenated into a SQL query; boolean and time-based payloads change the response.

The search endpoint on api.acme.example builds its query by concatenating the q parameter. A benign marker containing a single quote returns a database syntax error that echoes the marker, confirming the input reaches the query unescaped.

Root cause (insecure_code): The query is built by string concatenation instead of parameter binding.

BUSINESS IMPACT

Read and modify the application database.

Unescaped input in a SQL statement lets an attacker read or change data in the application database and, depending on privileges, run further statements.

LIKELIHOOD AND EXPLOITABILITY

Confidence High, likelihood likely; KEV listing not available. Error-based confirmation shows the input reaches the query, and the endpoint is unauthenticated, so likelihood is high.

AV
N

AC
L

PR
N

UI
N

S
U

C
H

I
H

A
H

CVSS vector CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H.

EVIDENCE

Observed 26 Sep 2026 17:56 UTC in web

notes: Error-based confirmation only; no timing or data-extraction probe was run.
request: GET /search?q=AQIRA-MARKER-sqli'
response: HTTP 500 – SQLSTATE 42601 syntax error near AQIRA-MARKER-sqli

REPRODUCTION STEPS

Preconditions: Network reach to https://api.acme.example/search

1. Send the marker with a trailing quote GET https://api.acme.example/search?q=AQIRA-MARKER-sqli'
 Expected: HTTP 500 with a SQL syntax error echoing the marker
2. Send the marker without the quote GET https://api.acme.example/search?q=AQIRA-MARKER-sqli
 Expected: HTTP 200, confirming the quote caused the error

PROOF OF CONCEPT (BENIGN)

Kind http
Title Error-based confirmation
Request GET https://api.acme.example/search?q=AQIRA-MARKER-sqli'
Response HTTP 500; body: SQLSTATE 42601 syntax error near AQIRA-MARKER-sqli
Marker AQIRA-MARKER-sqli
Notes A single unbalanced quote on the marker returns a syntax error that echoes the marker. No timing probe and no data-extraction payload were used.

REMEDIATION

Use parameterised queries and least-privilege database credentials.

1. Add a WAF rule as an interim control (contain, low effort, P1)
2. Rewrite the query to use bound parameters (fix, medium effort, P0)

```
var ps = conn.prepareStatement("SELECT id FROM items WHERE name = ?");
ps.setString(1, q);
```

3. Run the app with a least-privilege database account (harden, medium effort, P2)

Tier: Immediate (rank 2); effort Medium (template).

VERIFICATION

Retest status: not_retested

1. Re-send the quoted marker
 Expected: HTTP 200 with no SQL error

ATT&CK MITIGATIONS

- M1016 Vulnerability Scanning: Regularly scan externally facing systems for vulnerabilities and establish procedures to rapidly patch systems when critical vulnerabilities are discovered through scanning and through public disclosure.
- M1026 Privileged Account Management: Use least privilege for service accounts will limit what permissions the exploited process gets on the rest of the system.
- M1030 Network Segmentation: Segment externally facing servers and services from the rest of the network with a DMZ or on separate hosting infrastructure.
- M1048 Application Isolation and Sandboxing: Application isolation will limit what other processes and system features the exploited target can access.
- M1050 Exploit Protection: Web Application Firewalls may be used to limit exposure of applications to prevent exploit traffic from reaching the application.
- M1051 Update Software: Update software regularly by employing patch management for externally exposed applications.

ATT&CK DETECTION

- Application Log / Application Log Content: Detecting software exploitation may be difficult depending on the tools available. Software exploits may not always succeed or may cause the exploited process to become unstable or crash.
- Network Traffic / Network Traffic Content: Use deep packet inspection to look for artifacts of common exploit traffic, such as SQL injection strings or known payloads.

DETECTION

- Application Log / Application Log Content: Database syntax errors correlated with request parameter values.

ATT&CK

T1190 Exploit Public-Facing Application: Initial Access

CONTROLS

- **owasp** A03:2021 Injection
- **nistcsf** PR.PS-06 Secure software development practices are integrated, and their performance is monitored throughout the software development life cycle
- **nistcsf** ID.RA-01 Vulnerabilities in assets are identified, validated, and recorded
- **nist80053** SI-10 Information Input Validation
- **nist80053** SA-11 Developer Testing and Evaluation
- **nist800171** 3.14.1 Identify, report, and correct system flaws in a timely manner.
- **nist800171** 3.13.2 Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.
- **cobit** BAI03 Managed Solutions Identification and Build
- **cobit** DSS05 Managed Security Services

REFERENCES

- CWE-89
- ATT&CK T1190 Exploit Public-Facing Application (Initial Access)
- CWE-89
- ATT&CK T1190
- A03:2021 Injection
- SQL Injection Prevention Cheat Sheet

Lifecycle

When	From	To	By	Note
27 Aug 2026 14:14 UTC	created	Open	engine	n/a
29 Aug 2026 14:14 UTC	Open	Accepted risk	operator	Risk accepted for 30 days while the vendor patch is validated in staging.
14 Sep 2026 14:16 UTC	Accepted risk	Open	operator	Reopened: the follow-up assessment observed the issue again.

Internet facing

PCI scope

Quick win

F-03 Apache HTTP Server path traversal

High

Open

CVSS 7.5 Confidence High External Persisting from the previous run First seen 5 Sep 2026 14:19 UTC

Last seen 30 Sep 2026 02:00 UTC AQ-000025

Affected asset: https/443 tomcat (also observed in 13 other runs)
Locations: https://api.initech.example/cgi-bin/; api.initech.example:443

SUMMARY

Apache httpd 2.4.49 normalises paths incorrectly, letting a request read files outside the document root.

The server on www.initech.example reports Apache/2.4.49, a build whose path normalisation escapes the CGI directory. A request for a benign marker file placed one level up resolves outside the intended root, confirming the normalisation defect.

Root cause (missing_patch): Apache httpd 2.4.49 is deployed; the normalisation fix shipped in 2.4.51.

BUSINESS IMPACT

Disclosure of configuration files and, with CGI enabled, remote code execution.

An attacker can read files the web server can access outside the document root, exposing configuration and, where CGI is enabled, extend to command execution.

LIKELIHOOD AND EXPLOITABILITY

Confidence High, likelihood likely; KEV listing not available. The version is a known-defective build and the read is unauthenticated, so exposure is likely.

AV

AC

PR

UI

S

C

I

A

N

L

N

N

U

H

N

N

CVSS vector CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N.

EVIDENCE

Observed 26 Sep 2026 17:56 UTC in exploit

request: GET /cgi-bin/.%2e/AQIRA-MARKER-traversal.txt
version: Server: Apache/2.4.49 (Unix)
response: HTTP 200 – path normalisation escaped the CGI root; body contains AQIRA-MARKER-traversal

REPRODUCTION STEPS

Preconditions: Network reach to https://api.initech.example; A marker file placed one level above the CGI root on the demo host

1. Confirm the server version GET https://api.initech.example/ (read the Server header)
Expected: Apache/2.4.49
2. Request the marker through an encoded traversal GET https://api.initech.example/cgi-bin/.%2e/AQIRA-MARKER-traversal.txt
Expected: HTTP 200 with body AQIRA-MARKER-traversal

PROOF OF CONCEPT (BENIGN)

Kind	http
Title	Marker file read
Request	GET https://api.initech.example/cgi-bin/.%2e/AQIRA-MARKER-traversal.txt
Response	HTTP 200; body: AQIRA-MARKER-traversal
Marker	AQIRA-MARKER-traversal
Notes	The demo host serves a harmless marker file one directory above the CGI root. Reaching it confirms the normalisation defect without reading any sensitive file.

REMEDIATION

- Upgrade Apache HTTP Server to 2.4.51 or later and ensure 'Require all denied' protects the filesystem root.
1. Upgrade Apache HTTP Server to 2.4.51 or later (fix, medium effort, P0)

2. Add 'Require all denied' on the filesystem root (harden, low effort, P1)

```
<Directory />
  Require all denied
</Directory>
```

Tier: Immediate (rank 4); effort Medium (template); fixed in Apache HTTP Server 2.4.51.

VERIFICATION

Retest status: not_retested

1. Re-request the marker path

Expected: HTTP 403 or 404

2. Re-read the Server header

Expected: 2.4.51 or later

ATT&CK MITIGATIONS

- M1016 Vulnerability Scanning: Regularly scan externally facing systems for vulnerabilities and establish procedures to rapidly patch systems when critical vulnerabilities are discovered through scanning and through public disclosure.
- M1026 Privileged Account Management: Use least privilege for service accounts will limit what permissions the exploited process gets on the rest of the system.
- M1030 Network Segmentation: Segment externally facing servers and services from the rest of the network with a DMZ or on separate hosting infrastructure.
- M1048 Application Isolation and Sandboxing: Application isolation will limit what other processes and system features the exploited target can access.
- M1050 Exploit Protection: Web Application Firewalls may be used to limit exposure of applications to prevent exploit traffic from reaching the application.
- M1051 Update Software: Update software regularly by employing patch management for externally exposed applications.

ATT&CK DETECTION

- Application Log / Application Log Content: Detecting software exploitation may be difficult depending on the tools available. Software exploits may not always succeed or may cause the exploited process to become unstable or crash.
- Network Traffic / Network Traffic Content: Use deep packet inspection to look for artifacts of common exploit traffic, such as SQL injection strings or known payloads.

DETECTION

- Application Log / Web Credential: Access-log entries containing encoded dot-dot sequences such as `.%2e` or `%2e%2e`.

ATT&CK

T1190 Exploit Public-Facing Application: Initial Access

CONTROLS

- **owasp** A01:2021 Broken Access Control
- **owasp** A06:2021 Vulnerable and Outdated Components
- **nistcsf** ID.RA-01 Vulnerabilities in assets are identified, validated, and recorded
- **nistcsf** PR.PS-02 Software is maintained, replaced, and removed commensurate with risk
- **nist80053** SI-2 Flaw Remediation
- **nist80053** SI-10 Information Input Validation
- **nist80053** RA-5 Vulnerability Monitoring and Scanning
- **nist800171** 3.14.1 Identify, report, and correct system flaws in a timely manner.

- **nist800171** 3.11.3 Remediate vulnerabilities in accordance with risk assessments.
- **cobit** APO12 Managed Risk
- **cobit** DSS05 Managed Security Services

REFERENCES

- CVE-2021-41773
- CWE-22
- ATT&CK T1190 Exploit Public-Facing Application (Initial Access)
- CVE-2021-41773
- CWE-22
- ATT&CK T1190

Lifecycle

When	From	To	By	Note
5 Sep 2026 14:19 UTC	created	Open	engine	n/a
21 Sep 2026 17:03 UTC	Open	Resolved	operator	Verified fixed by the follow-up assessment.
23 Sep 2026 17:03 UTC	Resolved	Open	engine	Reopened: a later assessment observed the issue again.

Internet facing

PCI scope

Vendor patch required

F-04 Default credentials accepted on management service

High

False positive

CVSS 8.8 Confidence High External Persisting from the previous run First seen 5 Sep 2026 14:22 UTC
Last seen 28 Sep 2026 06:57 UTC AQ-000027

Affected asset: https/443 tomcat (also observed in 3 other runs)
Locations: https://api.acme.example/monitoring

SUMMARY

A management interface accepted the vendor's documented default username and password.

A monitoring console on api.acme.example still accepts the vendor's documented default account. The credential identifier is shown; the secret is masked in evidence.

Root cause (weak_identity): A vendor default account was left enabled with its documented password.

BUSINESS IMPACT

Full administrative control of the device.

The default account grants administrative control of the monitoring console and whatever it can reach.

LIKELIHOOD AND EXPLOITABILITY

Confidence High, likelihood likely; KEV listing not available. Default credentials are the first thing tried against a management surface, so likelihood is high.

AVN

ACL

PRN

UIN

SU

CH

IH

AH

CVSS vector CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H.

EVIDENCE

Observed 26 Sep 2026 17:56 UTC in web

```
login: admin / **** -> HTTP 200, session issued
service: management console
```

REPRODUCTION STEPS

Preconditions: Network reach to <https://api.acme.example/monitoring>

1. Open the monitoring console sign-in GET <https://api.acme.example/monitoring>
Expected: A vendor sign-in page
2. Confirm the default account is still enabled
The vendor default identifier authenticates; the secret is masked in the record

PROOF OF CONCEPT (BENIGN)

Kind auth

Title Credential policy readout

Notes The identifier is recorded and the secret is masked. The finding records that a vendor default is accepted, not the secret itself.

Secret values are masked.

REMEDIATION

Change the credential, enforce a unique strong password, and put the service behind SSO.

1. Disable or rename the default account (contain, trivial effort, P0)
2. Set a unique strong credential and enable MFA (fix, low effort, P0)
3. Front the console with SSO and maintain a credential inventory (harden, medium effort, P2)

Tier: not actionable; effort Low (template).

VERIFICATION

Retest status: not_retested

1. Attempt the vendor default
Expected: Authentication is rejected

ATT&CK MITIGATIONS

- M1027 Password Policies: Applications and appliances that utilize default username and password should be changed immediately after the installation, and before deployment to a production environment.

ATT&CK DETECTION

- Logon Session / Logon Session Creation: Monitor for newly constructed logon behavior across default accounts that have been activated or logged into.
- User Account / User Account Authentication: Monitor for an attempt by a user to gain access to a network or computing resource, often by providing credentials.

DETECTION

- Logon Session / Logon Session Creation: Successful sign-ins using vendor default account names.

ATT&CK

T1078.001 Default Accounts: Initial Access, Persistence, Privilege Escalation, Defense Evasion

CONTROLS

- **owasp** A07:2021 Identification and Authentication Failures
- **owasp** A05:2021 Security Misconfiguration

- **nistcsf** PR.AA-01 Identities and credentials for authorized users, services, and hardware are managed by the organization
- **nistcsf** PR.AA-03 Users, services, and hardware are authenticated
- **nistcsf** PR.PS-01 Configuration management practices are established and applied
- **nist80053** IA-5 Authenticator Management
- **nist80053** IA-2 Identification and Authentication (Organizational Users)
- **nist80053** CM-6 Configuration Settings
- **nist800171** 3.5.2 Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems.
- **nist800171** 3.5.3 Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.
- **nist800171** 3.4.2 Establish and enforce security configuration settings for information technology products employed in organizational systems.
- **cobit** DSS05 Managed Security Services
- **cobit** APO13 Managed Security

REFERENCES

- CWE-1392
- CWE-798
- ATT&CK T1078.001 Default Accounts (Initial Access, Persistence, Privilege Escalation, Defense Evasion)
- CWE-1392
- ATT&CK T1078.001

Lifecycle

When	From	To	By	Note
5 Sep 2026 14:22 UTC	created	Open	engine	n/a
22 Sep 2026 17:03 UTC	Open	False positive	operator	Banner is spoofed by the load balancer.

Internet facing

PCI scope

Vendor patch required

F-05 Source control metadata exposed (.git directory)

High

Open

CVSS 7.5 Confidence High External Persisting from the previous run First seen 14 Sep 2026 14:24 UTC
Last seen 26 Sep 2026 17:56 UTC AQ-000035

Affected asset: admin.acme.example (also observed in 1 other run)
Locations: https://admin.acme.example/.git/HEAD

SUMMARY

The web root serves the .git directory, allowing the full source history to be reconstructed.

The web root on www.acme.example serves the .git directory. Its metadata lets the full source history, including anything committed to it, be reconstructed.

Root cause (misconfiguration): The deployment artefact includes the .git directory and the web server serves dot-paths.

BUSINESS IMPACT

Source code and committed secrets disclosed.

The repository history can be rebuilt from the exposed metadata, disclosing source code and any secrets committed to it.

LIKELIHOOD AND EXPLOITABILITY

Confidence High, likelihood likely; KEV listing not available. The path is reachable with a single request and the reconstruction is well known, so likelihood is high.

AV
N

AC
L

PR
N

UI
N

S
U

C
H

I
N

A
N

CVSS vector CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N.

EVIDENCE

Observed 26 Sep 2026 17:56 UTC in web

url: https://acme.example/.git/HEAD

body: ref: refs/heads/main

Observed 26 Sep 2026 17:56 UTC in web

url: https://acme.example/.git/HEAD

body: ref: refs/heads/main

REPRODUCTION STEPS

Preconditions: Network reach to https://admin.acme.example

1. Request the repository HEAD file GET https://admin.acme.example/.git/HEAD
- Expected: HTTP 200 with a ref line

PROOF OF CONCEPT (BENIGN)

Kind	http
Title	Metadata reachability check
Request	GET https://admin.acme.example/.git/HEAD
Response	HTTP 200; body: ref: refs/heads/main
Notes	A single read of the HEAD file confirms the metadata is served. No history is downloaded.

REMEDIATION

Remove .git from the deployed artefact and deny dot-paths at the web server.

1. Deny access to /.git at the web server (contain, trivial effort, P0)
2. Remove the .git directory from the deployed artefact (fix, low effort, P0)
3. Deny all dotfiles by default and rotate any committed secrets (harden, medium effort, P1)

Tier: Immediate (rank 5); effort Low (template).

VERIFICATION

Retest status: not_retested

1. Re-request /.git/HEAD
- Expected: HTTP 404 or 403

ATT&CK MITIGATIONS

- M1017 User Training: Develop and publish policies that define acceptable information to be stored in code repositories.
- M1018 User Account Management: Enforce the principle of least-privilege. Consider implementing access control mechanisms that include both authentication and authorization for code repositories.
- M1032 Multi-factor Authentication: Use multi-factor authentication for logons to code repositories.
- M1047 Audit: Consider periodic reviews of accounts and privileges for critical and sensitive code repositories. Scan code repositories for exposed credentials or other sensitive information.

ATT&CK DETECTION

- Application Log / Application Log Content: Monitor for third-party application logging, messaging, and/or other artifacts that may leverage code repositories to collect valuable information.
- Logon Session / Logon Session Creation: Monitor for newly constructed logon behavior across code repositories (e.g. Github) which can be configured to report access to certain pages and documents.

DETECTION

- Application Log / Web Credential: Access-log requests for /.git/ paths.

ATT&CK

T1213.003 Code Repositories: Collection

CONTROLS

- **owasp** A05:2021 Security Misconfiguration
- **owasp** A01:2021 Broken Access Control
- **nistcsf** PR.PS-01 Configuration management practices are established and applied
- **nistcsf** PR.PS-06 Secure software development practices are integrated, and their performance is monitored throughout the software development life cycle
- **nist80053** CM-7 Least Functionality
- **nist80053** CM-6 Configuration Settings
- **nist800171** 3.4.2 Establish and enforce security configuration settings for information technology products employed in organizational systems.
- **nist800171** 3.4.7 Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.
- **cobit** BAI10 Managed Configuration
- **cobit** DSS05 Managed Security Services

REFERENCES

- CWE-538
- CWE-540
- ATT&CK T1213.003 Code Repositories (Collection)
- CWE-538
- ATT&CK T1213.003

Lifecycle

When	From	To	By	Note
14 Sep 2026 14:24 UTC	created	Open	engine	n/a

Internet facing

F-06 Dangling DNS record allows subdomain takeover

High

[Open](#)

CVSS 8.2 Confidence Medium External Persisting from the previous run First seen 27 Aug 2026 14:16 UTC
Last seen 26 Sep 2026 17:56 UTC AQ-000004

Affected asset: status.acme.example (also observed in 2 other runs)
Locations: status.acme.example

SUMMARY

A CNAME points to an unclaimed cloud resource that anyone can register.

status.acme.example is a CNAME to a platform resource that no longer exists. Because the target is unclaimed, whoever registers it next controls content served from the trusted subdomain.

Root cause (process_gap): A DNS record was left pointing at a decommissioned resource.

BUSINESS IMPACT

Phishing and cookie theft from a trusted subdomain.

An attacker who claims the dangling target serves their own content from the organisation's subdomain, enabling convincing phishing and theft of cookies scoped to the domain.

LIKELIHOOD AND EXPLOITABILITY

Confidence Medium, likelihood possible; KEV listing not available. The record is dangling now, but takeover requires claiming the target, so likelihood is possible.

AV N	AC L	PR N	UI N	S C	C L	I H	A N
---------	---------	---------	---------	--------	--------	--------	--------

CVSS vector CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:H/A:N.

EVIDENCE

Observed 26 Sep 2026 17:56 UTC in recon

record: status.acme.example CNAME unclaimed-app.paas.example
response: The target responds: no such application

REPRODUCTION STEPS

Preconditions: Public DNS resolution for acme.example

1. Resolve the subdomain `dig status.acme.example CNAME`
Expected: A CNAME to unclaimed-app.paas.example
2. Request the target `GET the CNAME target`
Expected: A not-found response indicating the target is unclaimed

PROOF OF CONCEPT (BENIGN)

Kind dns

Title Dangling CNAME readout

Notes The record and the target's not-found response are read. No resource is registered.

REMEDIATION

Delete the stale record or reclaim the target resource.

1. Remove the dangling DNS record (contain, trivial effort, P0)
2. Reclaim or repoint the target resource if the subdomain is still needed (fix, low effort, P1)
3. Run a periodic DNS hygiene job to catch dangling records (harden, medium effort, P2)

Tier: Short term (rank 1); effort Low (template).

VERIFICATION

Retest status: not_retested

1. Re-resolve the subdomain
Expected: The record is gone or resolves to a claimed resource

ATT&CK MITIGATIONS

- M1056 Pre-compromise: This technique cannot be easily mitigated with preventive controls since it is based on behaviors performed outside of the scope of enterprise defenses and controls.

ATT&CK DETECTION

- Domain Name / Active DNS: Monitor for queried domain name system (DNS) registry data that may hijack domains and/or subdomains that can be used during targeting.
- Domain Name / Domain Registration: Consider monitoring for anomalous changes to domain registrant information and/or domain resolution information that may indicate the compromise of a domain.
- Domain Name / Passive DNS: Monitor for logged domain name system (DNS) registry data that may hijack domains and/or subdomains that can be used during targeting.

DETECTION

- Domain Name / Domain Registration: DNS records whose targets return not-found or unclaimed responses.

ATT&CK

T1584.001 Domains: Resource Development

CONTROLS

- **owasp** A05:2021 Security Misconfiguration
- **nistcsf** ID.AM-02 Inventories of software, services, and systems managed by the organization are maintained
- **nistcsf** ID.AM-08 Systems, hardware, software, services, and data are managed throughout their life cycles
- **nist80053** CM-8 System Component Inventory
- **nist80053** CM-6 Configuration Settings
- **nist800171** 3.4.1 Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.
- **cobit** BAI09 Managed Assets
- **cobit** BAI10 Managed Configuration

REFERENCES

- CWE-284
- ATT&CK T1584.001 Domains (Resource Development)
- CWE-284
- ATT&CK T1584.001

Lifecycle

When	From	To	By	Note
27 Aug 2026 14:16 UTC	created	Open	engine	n/a

Internet facing

F-07 Publicly listable cloud storage bucket

High

[Open](#)

CVSS 7.5 Confidence High External Persisting from the previous run First seen 27 Aug 2026 14:22 UTC
Last seen 26 Sep 2026 17:56 UTC AQ-000010

Affected asset: acme.example-assets (also observed in 3 other runs)
Locations: acme.example-assets

SUMMARY

A storage bucket referenced by the site allows anonymous ListBucket.

A storage bucket referenced by acme.example answers an anonymous list request, returning an object count. Anonymous enumeration exposes what the bucket holds to anyone.

Root cause (misconfiguration): The bucket permits anonymous list access instead of blocking public access.

BUSINESS IMPACT

Exposure of backups and internal documents.
Anonymous listing reveals object names and counts, and any object whose read is also public can be retrieved.

LIKELIHOOD AND EXPLOITABILITY

Confidence High, likelihood likely; KEV listing not available. The bucket is referenced by the public site and lists anonymously, so exposure is likely.

AVN

ACL

PRN

UIN

SU

CH

IN

ANN

CVSS vector CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N.

EVIDENCE

Observed 26 Sep 2026 17:56 UTC in infra

url: https://acme.example-assets.storage.example/?list-type=2
objects: 1834

REPRODUCTION STEPS

Preconditions: The bucket endpoint is reachable without credentials

1. Request an anonymous object listing GET https://acme.example-assets.storage.example/?list-type=2
- Expected: HTTP 200 with an object listing

PROOF OF CONCEPT (BENIGN)

Kind	http
Title	Anonymous list check
Request	GET https://acme.example-assets.storage.example/?list-type=2
Response	HTTP 200; a listing enumerating objects (count only recorded: 1834)
Notes	A single read-only list request confirms anonymous enumeration. Only the object count is recorded; no object is downloaded.

REMEDIATION

Block public access on the bucket and serve assets through a CDN origin access identity.

1. Enable block-public-access on the bucket (contain, trivial effort, P0)
2. Scope the bucket policy to least privilege (fix, low effort, P1)
3. Serve public assets through a CDN with an origin access identity and enable access logging (harden, medium effort, P2)

Tier: Immediate (rank 6); effort Low (template).

VERIFICATION

Retest status: not_retested

1. Repeat the anonymous list request
- Expected: HTTP 403

ATT&CK MITIGATIONS

- M1018 User Account Management: Configure user permissions groups and roles for access to cloud storage. Implement strict Identity and Access Management (IAM) controls to prevent access to storage

solutions except for the applications, users, and services that require access.

- M1022 Restrict File and Directory Permissions: Use access control lists on storage systems and objects.
- M1032 Multi-factor Authentication: Consider using multi-factor authentication to restrict access to resources and cloud storage APIs.
- M1037 Filter Network Traffic: Cloud service providers support IP-based restrictions when accessing cloud resources.
- M1041 Encrypt Sensitive Information: Encrypt data stored at rest in cloud storage. Managed encryption keys can be rotated by most providers. At a minimum, ensure an incident response plan to storage breach includes rotating the keys and test for impact on client applications.
- M1047 Audit: Frequently check permissions on cloud storage to ensure proper permissions are set to deny open or unprivileged access to resources.

ATT&CK DETECTION

- Cloud Storage / Cloud Storage Access: Monitor for unusual queries to the cloud provider's storage service. Activity originating from unexpected sources may indicate improper permissions are set and are allowing access to data.

DETECTION

- Cloud Storage / Cloud Storage Access: Anonymous or unauthenticated list operations against storage buckets.

ATT&CK

T1530 Data from Cloud Storage: Collection

CONTROLS

- **owasp** A01:2021 Broken Access Control
- **owasp** A05:2021 Security Misconfiguration
- **nistcsf** PR.DS-01 The confidentiality, integrity, and availability of data-at-rest are protected
- **nistcsf** PR.AA-05 Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties
- **nist80053** AC-3 Access Enforcement
- **nist80053** AC-6 Least Privilege
- **nist80053** AC-22 Publicly Accessible Content
- **nist800171** 3.1.1 Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).
- **nist800171** 3.1.22 Control CUI posted or processed on publicly accessible systems.
- **cobit** DSS05 Managed Security Services
- **cobit** APO14 Managed Data

REFERENCES

- CWE-732
- CWE-284
- ATT&CK T1530 Data from Cloud Storage (Collection)
- CWE-732
- ATT&CK T1530
- A01:2021 Broken Access Control

Lifecycle

When	From	To	By	Note
27 Aug 2026 14:22 UTC	created	Open	engine	n/a

When	From	To	By	Note
29 Aug 2026 14:22 UTC	Open	Accepted risk	operator	Risk accepted for 30 days while the vendor patch is validated in staging.
14 Sep 2026 14:22 UTC	Accepted risk	Open	operator	Reopened: the follow-up assessment observed the issue again.

Internet facing

Quick win

F-08 Database port reachable from the internet

High

Open

CVSS 8.1 Confidence High External Persisting from the previous run First seen 27 Aug 2026 14:13 UTC
Last seen 26 Sep 2026 17:44 UTC AQ-000001

Affected asset: admin.acme.example (also observed in 3 other runs)
Locations: admin.acme.example:5432

SUMMARY

PostgreSQL (5432/tcp) accepts connections from any source address.

The database port on api.acme.example answers from any source address, exposing the service banner and inviting direct connection attempts against the data tier.

Root cause (exposed_service): The database listener is bound to a public interface with no network restriction.

BUSINESS IMPACT

Direct brute force and exploitation of the database.
The database is reachable from the internet, so it can be attacked directly rather than only through the application.

LIKELIHOOD AND EXPLOITABILITY

Confidence High, likelihood likely; KEV listing not available. A directly reachable data tier is routinely scanned and probed, so likelihood is high.

AV
N

AC
L

PR
N

UI
N

S
U

C
H

I
L

A
L

CVSS vector CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:L.

EVIDENCE

Observed 26 Sep 2026 17:44 UTC in recon

port: 5432/tcp open
banner: PostgreSQL 13.4

REPRODUCTION STEPS

Preconditions: A source address outside any corporate network

1. Connect to the database port TCP connect to admin.acme.example:5432
Expected: The port is open and returns a banner

PROOF OF CONCEPT (BENIGN)

Kind service

Title Open-port readout

Request TCP connect to admin.acme.example:5432

Response Port open; banner PostgreSQL 13.4

Notes A connection confirms the port answers and reads the version banner. No authentication is attempted.

REMEDIATION

Bind the database to private interfaces and restrict with security groups.

1. Restrict the port with a security group or firewall rule (contain, low effort, P0)
2. Bind the database to a private interface or subnet (fix, medium effort, P1)
3. Segment the data tier from the public network (harden, high effort, P2)

Tier: Immediate (rank 3); effort Medium (template).

VERIFICATION

Retest status: not_retested

1. Re-scan the port from outside

Expected: The port is filtered

ATT&CK MITIGATIONS

- M1030 Network Segmentation: Ensure proper network segmentation is followed to protect critical servers and devices.
- M1031 Network Intrusion Prevention: Use network intrusion detection/prevention systems to detect and prevent remote service scans.
- M1042 Disable or Remove Feature or Program: Ensure that unnecessary ports and services are closed to prevent risk of discovery and potential exploitation.

ATT&CK DETECTION

- Cloud Service / Cloud Service Enumeration: Cloud service discovery techniques will likely occur throughout an operation where an adversary is targeting cloud-based systems and services.
- Command / Command Execution: Monitor executed commands and arguments that may attempt to get a listing of services running on remote hosts, including those that may be vulnerable to remote software exploitation.
- Network Traffic / Network Traffic Flow: Monitor network data for uncommon data flows. Processes utilizing the network that do not normally have network communication or have never been seen before are suspicious.

DETECTION

- Network Traffic / Network Connection Creation: Inbound connections to database ports from external addresses.

ATT&CK

T1046 Network Service Discovery: Discovery

CONTROLS

- **owasp** A05:2021 Security Misconfiguration
- **nistcsf** PR.IR-01 Networks and environments are protected from unauthorized logical access and usage
- **nistcsf** DE.CM-01 Networks and network services are monitored to find potentially adverse events
- **nist80053** SC-7 Boundary Protection
- **nist80053** CM-7 Least Functionality
- **nist800171** 3.13.1 Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.
- **nist800171** 3.13.5 Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.
- **nist800171** 3.4.7 Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.

- **cobit** DSS05 Managed Security Services
- **cobit** BAI10 Managed Configuration

REFERENCES

- CWE-284
- CWE-668
- ATT&CK T1046 Network Service Discovery (Discovery)
- CWE-284
- ATT&CK T1046

Lifecycle

When	From	To	By	Note
27 Aug 2026 14:13 UTC	created	Open	engine	n/a
29 Aug 2026 14:13 UTC	Open	Accepted risk	operator	Risk accepted for 30 days while the vendor patch is validated in staging.
14 Sep 2026 14:14 UTC	Accepted risk	Open	operator	Reopened: the follow-up assessment observed the issue again.

Internet facing

PCI scope

F-09 Outdated TLS protocol versions accepted

Medium

Open

CVSS 5.9 Confidence High External Persisting from the previous run First seen 5 Sep 2026 14:17 UTC
Last seen 28 Sep 2026 06:57 UTC AQ-000023

Affected asset: https/443 tomcat (also observed in 3 other runs)
Locations: api.acme.example:443

SUMMARY

The server negotiates TLS 1.0 and TLS 1.1, which are deprecated by RFC 8996.

The TLS endpoint on www.acme.example still offers TLS 1.0 and TLS 1.1 alongside 1.2. These versions are deprecated and permit weak CBC cipher suites, lowering the assurance of transport confidentiality.

Root cause (misconfiguration): Deprecated TLS versions remain enabled in the server configuration.

BUSINESS IMPACT

Downgrade and interception attacks against clients.

A network attacker able to influence the handshake can steer a client onto a deprecated version and a weak cipher, reducing confidentiality guarantees for the session.

LIKELIHOOD AND EXPLOITABILITY

Confidence High, likelihood possible; KEV listing not available. Exploitation needs a man-in-the-middle position, so likelihood is possible rather than likely.

AV N	AC H	PR N	UI N	S U	C H	I N	A N
---------	---------	---------	---------	--------	--------	--------	--------

CVSS vector CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N.

EVIDENCE

Observed 26 Sep 2026 17:56 UTC in infra

cipher: TLS_RSA_WITH_AES_128_CBC_SHA
protocols: TLSv1.0, TLSv1.1, TLSv1.2

REPRODUCTION STEPS

Preconditions: Network reach to the TLS port on api.acme.example

1. Enumerate supported protocol versions TLS handshake attempts for 1.0, 1.1, 1.2 and 1.3
Expected: 1.0 and 1.1 are accepted

PROOF OF CONCEPT (BENIGN)

Kind tls

Title Offered protocol readout

Notes A handshake enumeration lists the protocol versions and ciphers the server will accept.

REMEDIATION

Disable TLS 1.0/1.1 and offer only TLS 1.2 with AEAD suites and TLS 1.3.

1. Disable TLS 1.0 and TLS 1.1 (fix, low effort, P1)
2. Offer only AEAD cipher suites on TLS 1.2 and enable TLS 1.3 (harden, low effort, P2)
3. Add HSTS so clients refuse to downgrade (harden, low effort, P2)

Tier: Medium term (rank 2); effort Low (template).

VERIFICATION

Retest status: not_retested

1. Re-enumerate protocol versions
Expected: Only TLS 1.2 and 1.3 are accepted

ATT&CK MITIGATIONS

- M1017 User Training: Train users to be suspicious about certificate errors. Adversaries may use their own certificates in an attempt to intercept HTTPS traffic.
- M1030 Network Segmentation: Network segmentation can be used to isolate infrastructure components that do not require broad network access.
- M1031 Network Intrusion Prevention: Network intrusion detection and prevention systems that can identify traffic patterns indicative of AiTM activity can be used to mitigate activity at the network level.
- M1035 Limit Access to Resource Over Network: Limit access to network infrastructure and resources that can be used to reshape traffic or otherwise produce AiTM conditions.
- M1037 Filter Network Traffic: Use network appliances and host-based security software to block network traffic that is not necessary within the environment, such as legacy protocols that may be leveraged for AiTM conditions.
- M1041 Encrypt Sensitive Information: Ensure that all wired and/or wireless traffic is encrypted appropriately. Use best practices for authentication protocols, such as Kerberos, and ensure web traffic that may contain credentials is protected by SSL/TLS.
- M1042 Disable or Remove Feature or Program: Disable legacy network protocols that may be used to intercept network traffic if applicable, especially those that are not needed within an environment.

ATT&CK DETECTION

- Application Log / Application Log Content: Monitor application logs for changes to settings and other events associated with network protocols and other services commonly abused for AiTM.
- Network Traffic / Network Traffic Content: Monitor network traffic for anomalies associated with known AiTM behavior.

- **Network Traffic / Network Traffic Flow:** Monitor for network traffic originating from unknown/unexpected hardware devices. Local network traffic metadata (such as source MAC addressing) as well as usage of network management protocols such as DHCP may be helpful in identifying hardware.
- **Service / Service Creation:** Monitor for newly constructed services/daemons through Windows event logs for event IDs 4697 and 7045.

DETECTION

- **Network Traffic / Network Traffic Content:** TLS handshakes that negotiate 1.0 or 1.1.

ATT&CK

T1557 Adversary-in-the-Middle: Credential Access, Collection

CONTROLS

- **owasp** A02:2021 Cryptographic Failures
- **nistcsf** PR.DS-02 The confidentiality, integrity, and availability of data-in-transit are protected
- **nist80053** SC-8 Transmission Confidentiality and Integrity
- **nist80053** SC-13 Cryptographic Protection
- **nist800171** 3.13.8 Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.
- **cobit** DSS05 Managed Security Services

REFERENCES

- CWE-326
- CWE-327
- ATT&CK T1557 Adversary-in-the-Middle (Credential Access, Collection)
- CWE-326
- ATT&CK T1557
- Transport Layer Security Cheat Sheet

Lifecycle

When	From	To	By	Note
5 Sep 2026 14:17 UTC	created	Open	engine	n/a

Needs owner

PCI scope

F-10 Login portal does not enforce multi-factor authentication

Medium

[Open](#)

CVSS 6.5 Confidence Medium External Persisting from the previous run First seen 14 Sep 2026 14:17 UTC
Last seen 26 Sep 2026 17:56 UTC AQ-000034

Affected asset: admin.acme.example (also observed in 1 other run)
Locations: https://admin.acme.example/login

SUMMARY

The customer login accepts a password alone and applies no lockout after repeated failures.

The customer sign-in on www.acme.example accepts a password with no second factor and shows no lockout or challenge after repeated failed attempts, leaving accounts open to credential stuffing.

Root cause (misconfiguration): The portal enforces neither MFA nor lockout or rate limiting.

BUSINESS IMPACT

Credential stuffing yields account takeover.
With no second factor and no rate limit, reused or guessed passwords lead directly to account takeover.

LIKELIHOOD AND EXPLOITABILITY

Confidence Medium, likelihood likely; KEV listing not available. Credential stuffing against password-only portals is common and cheap, so likelihood is high.

AV

N

AC

L

PR

N

UI

N

S

U

C

H

I

N

A

N

CVSS vector CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N.

EVIDENCE

Observed 26 Sep 2026 17:56 UTC in web

attempts: Repeated failed sign-ins with no lockout or challenge

REPRODUCTION STEPS

Preconditions: Network reach to https://admin.acme.example/login; A test account or an invalid identifier

1. Submit several failed sign-ins for one identifier
- Expected: No lockout, delay or challenge appears
- Use an invalid password on a known-invalid identifier
2. Confirm no second factor is requested on success
- A valid password alone completes sign-in

PROOF OF CONCEPT (BENIGN)

Kind auth
Title Lockout policy readout
Notes The check observes only that repeated failures produce no lockout or challenge. No account is compromised.

REMEDIATION

Require MFA for all accounts and add progressive lockout / rate limiting.

1. Enable progressive lockout or rate limiting (contain, low effort, P1)
2. Require MFA for all accounts (fix, medium effort, P1)
3. Add conditional access and anomaly detection (harden, medium effort, P2)

Tier: Medium term (rank 1); effort Medium (template).

VERIFICATION

Retest status: not_retested

1. Repeat the failed sign-ins
- Expected: A lockout or challenge appears
2. Sign in with a valid password
- Expected: A second factor is requested

ATT&CK MITIGATIONS

- M1018 User Account Management: Proactively reset accounts that are known to be part of breached credentials either immediately, or after detecting bruteforce attempts.
- M1027 Password Policies: Refer to NIST guidelines when creating password policies.
- M1032 Multi-factor Authentication: Use multi-factor authentication. Where possible, also enable multi-factor authentication on externally facing services.
- M1036 Account Use Policies: Set account lockout policies after a certain number of failed login attempts to prevent passwords from being guessed.

ATT&CK DETECTION

- Application Log / Application Log Content: Monitor authentication logs for system and application login failures of Valid Accounts. If authentication failures are high, then there may be a brute force attempt to gain access to a system using legitimate credentials.
- User Account / User Account Authentication: Monitor for many failed authentication attempts across various accounts that may result from credential stuffing attempts.

DETECTION

- Logon Session / Logon Session Creation: High failure counts per account with no corresponding logout.

ATT&CK

T1110.004 Credential Stuffing: Credential Access

CONTROLS

- **owasp** A07:2021 Identification and Authentication Failures
- **nistcsf** PR.AA-03 Users, services, and hardware are authenticated
- **nistcsf** PR.AA-01 Identities and credentials for authorized users, services, and hardware are managed by the organization
- **nist80053** IA-2 Identification and Authentication (Organizational Users)
- **nist80053** AC-7 Unsuccessful Logon Attempts
- **nist800171** 3.5.3 Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.
- **nist800171** 3.1.8 Limit unsuccessful logon attempts.
- **cobit** DSS05 Managed Security Services

REFERENCES

- CWE-308
- CWE-307
- ATT&CK T1110.004 Credential Stuffing (Credential Access)
- CWE-308
- ATT&CK T1110.004
- Authentication Cheat Sheet

Lifecycle

When	From	To	By	Note
14 Sep 2026 14:17 UTC	created	Open	engine	n/a

Needs owner

F-11 Security headers missing (CSP, HSTS)

Low

Open

CVSS 3.1 Confidence High External Persisting from the previous run First seen 27 Aug 2026 14:24 UTC
Last seen 26 Sep 2026 17:56 UTC AQ-000012

Affected asset: admin.acme.example (also observed in 2 other runs)
Locations: https://admin.acme.example/

SUMMARY

Responses lack Content-Security-Policy and Strict-Transport-Security.

Responses from `www.acme.example` omit Content-Security-Policy and Strict-Transport-Security, so defence-in-depth against script injection and transport downgrade is weaker than it should be.

Root cause (misconfiguration): The response headers are not configured.

BUSINESS IMPACT

Weaker defence in depth against XSS and downgrade.
Without CSP a script-injection flaw is easier to exploit, and without HSTS a client can be downgraded to plaintext on first contact.

LIKELIHOOD AND EXPLOITABILITY

Confidence High, likelihood possible; KEV listing not available. These are defence-in-depth controls, so the impact is contributory rather than direct; likelihood is possible.

AV
N

AC
H

PR
N

UI
R

S
U

C
L

I
N

A
N

CVSS vector CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N.

EVIDENCE

Observed 26 Sep 2026 17:56 UTC in web

missing: content-security-policy, strict-transport-security

REPRODUCTION STEPS

Preconditions: Network reach to `https://admin.acme.example`

1. Read the response headers `GET https://admin.acme.example/` and inspect the headers
- Expected: No CSP and no HSTS header

PROOF OF CONCEPT (BENIGN)

Kind config
Title Missing header readout
Notes The response headers are read and compared against the expected set.

REMEDIATION

Add HSTS with a long max-age and a restrictive CSP.

1. Add a restrictive Content-Security-Policy in report-only mode (fix, low effort, P2)
2. Enable Strict-Transport-Security with a long max-age (fix, trivial effort, P2)
3. Move CSP from report-only to enforce after monitoring (harden, low effort, P3)

Tier: Next cycle (rank 2); effort Low (template).

VERIFICATION

Retest status: not_retested

1. Re-read the response headers
- Expected: CSP and HSTS are present

ATT&CK MITIGATIONS

- M1017 User Training: Train users to be suspicious about certificate errors. Adversaries may use their own certificates in an attempt to intercept HTTPS traffic.
- M1030 Network Segmentation: Network segmentation can be used to isolate infrastructure components that do not require broad network access.
- M1031 Network Intrusion Prevention: Network intrusion detection and prevention systems that can identify traffic patterns indicative of AiTM activity can be used to mitigate activity at the network level.

- **M1035 Limit Access to Resource Over Network:** Limit access to network infrastructure and resources that can be used to reshape traffic or otherwise produce AiTM conditions.
- **M1037 Filter Network Traffic:** Use network appliances and host-based security software to block network traffic that is not necessary within the environment, such as legacy protocols that may be leveraged for AiTM conditions.
- **M1041 Encrypt Sensitive Information:** Ensure that all wired and/or wireless traffic is encrypted appropriately. Use best practices for authentication protocols, such as Kerberos, and ensure web traffic that may contain credentials is protected by SSL/TLS.
- **M1042 Disable or Remove Feature or Program:** Disable legacy network protocols that may be used to intercept network traffic if applicable, especially those that are not needed within an environment.

ATT&CK DETECTION

- **Application Log / Application Log Content:** Monitor application logs for changes to settings and other events associated with network protocols and other services commonly abused for AiTM.
- **Network Traffic / Network Traffic Content:** Monitor network traffic for anomalies associated with known AiTM behavior.
- **Network Traffic / Network Traffic Flow:** Monitor for network traffic originating from unknown/unexpected hardware devices. Local network traffic metadata (such as source MAC addressing) as well as usage of network management protocols such as DHCP may be helpful in identifying hardware.
- **Service / Service Creation:** Monitor for newly constructed services/daemons through Windows event logs for event IDs 4697 and 7045.

DETECTION

- **Application Log / Application Log Content:** Responses served without the expected security headers.

ATT&CK

T1557 Adversary-in-the-Middle: Credential Access, Collection

CONTROLS

- **owasp** A05:2021 Security Misconfiguration
- **nistcsf** PR.PS-01 Configuration management practices are established and applied
- **nist80053** CM-6 Configuration Settings
- **nist80053** SC-8 Transmission Confidentiality and Integrity
- **nist800171** 3.4.2 Establish and enforce security configuration settings for information technology products employed in organizational systems.
- **nist800171** 3.13.8 Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.
- **cobit** BAI10 Managed Configuration

REFERENCES

- CWE-693
- CWE-1021
- ATT&CK T1557 Adversary-in-the-Middle (Credential Access, Collection)
- CWE-693
- ATT&CK T1557
- HTTP Security Response Headers Cheat Sheet

Lifecycle

When	From	To	By	Note
27 Aug 2026 14:24 UTC	created	Open	engine	n/a

Quick win

F-12 Directory listing enabled

Low

Open

CVSS 3.7 Confidence High External Persisting from the previous run First seen 27 Aug 2026 14:20 UTC
Last seen 26 Sep 2026 17:28 UTC AQ-000008

Affected asset: admin.acme.example (also observed in 2 other runs)
Locations: https://admin.acme.example/uploads/

SUMMARY

The /uploads/ path returns an auto-generated index of files.

The /uploads/ path on www.acme.example returns an auto-generated file index, letting anyone enumerate the files stored there.

Root cause (misconfiguration): Automatic directory indexing is enabled on the uploads path.

BUSINESS IMPACT

Enumeration of uploaded files.

An index of uploaded files lets an attacker enumerate and retrieve content that was meant to be reached only by direct link.

LIKELIHOOD AND EXPLOITABILITY

Confidence High, likelihood possible; KEV listing not available. The listing is public but the sensitivity depends on what is stored, so likelihood is possible.

AV
N

AC
L

PR
N

UI
N

S
U

C
L

I
N

A
N

CVSS vector CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N.

EVIDENCE

Observed 26 Sep 2026 17:28 UTC in web

url: https://acme.example/uploads/
title: Index of /uploads

REPRODUCTION STEPS

Preconditions: Network reach to https://admin.acme.example

1. Request the uploads directory GET https://admin.acme.example/uploads/
Expected: An "Index of /uploads" page

PROOF OF CONCEPT (BENIGN)

Kind http

Title Directory index check

Request GET https://admin.acme.example/uploads/

Response HTTP 200; page title "Index of /uploads"

Notes A single read confirms the auto-generated index is served.

REMEDIATION

Disable autoindex and serve uploads through signed URLs.

1. Disable automatic directory indexing (fix, trivial effort, P2)

2. Serve uploads through signed, time-limited URLs (harden, medium effort, P3)

Tier: Next cycle (rank 1); effort Low (template).

VERIFICATION

Retest status: not_retested

1. Re-request the uploads path
- Expected: No index is returned

ATT&CK MITIGATIONS

- M1056 Pre-compromise: This technique cannot be easily mitigated with preventive controls since it is based on behaviors performed outside of the scope of enterprise defenses and controls.

ATT&CK DETECTION

- Application Log / Application Log Content: Monitor for suspicious network traffic that could be indicative of adversary reconnaissance, such as rapid successions of requests indicative of web crawling and/or large quantities of requests originating from a single source (especially if the source is...

DETECTION

- Application Log / Application Log Content: Requests to directory paths that return generated index pages.

ATT&CK

T1594 Search Victim-Owned Websites: Reconnaissance

CONTROLS

- **owasp** A05:2021 Security Misconfiguration
- **owasp** A01:2021 Broken Access Control
- **nistcsf** PR.PS-01 Configuration management practices are established and applied
- **nist80053** CM-7 Least Functionality
- **nist80053** CM-6 Configuration Settings
- **nist800171** 3.4.6 Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.
- **nist800171** 3.4.7 Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.
- **cobit** BAI10 Managed Configuration

REFERENCES

- CWE-548
- ATT&CK T1594 Search Victim-Owned Websites (Reconnaissance)
- CWE-548
- ATT&CK T1594

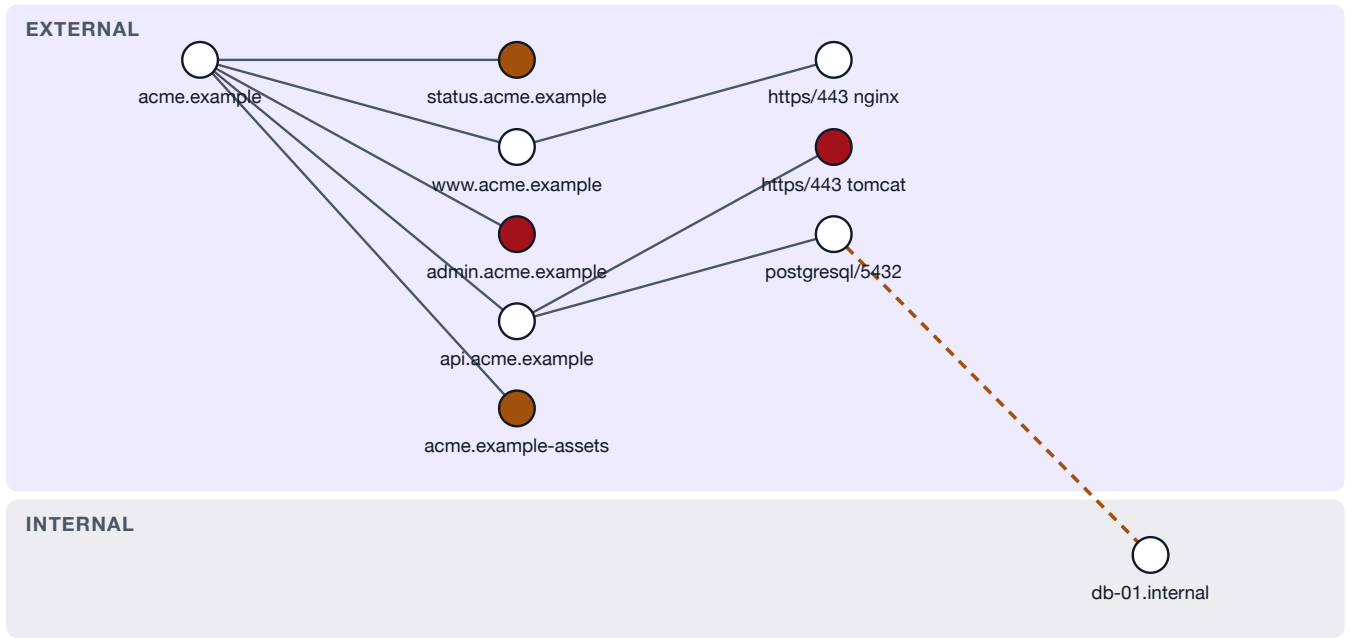
Lifecycle

When	From	To	By	Note
27 Aug 2026 14:20 UTC	created	Open	engine	n/a
29 Aug 2026 14:20 UTC	Open	Accepted risk	operator	Risk accepted for 30 days while the vendor patch is validated in staging.
14 Sep 2026 14:13 UTC	Accepted risk	Open	operator	Reopened: the follow-up assessment observed the issue again.

Quick win

9. Attack surface and asset inventory

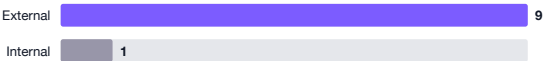
10 assets were recorded: 9 externally reachable and 1 internal, linked by 9 relationships of which 1 cross the exposure boundary.



Topology: external lane above, internal below; dashed links cross the boundary, node colour is the worst finding severity.



Assets by kind.



Assets by exposure.

Asset inventory

Kind	Label	Address	Exposure	Found in	Linked from	Worst	Findings	Seen
domain	acme.example	n/a	External	recon	root	none	0	Known (4 runs)
dns	status.acme.example	n/a	External	recon	acme.example (resolves)	High	1	Known (4 runs)
host	www.acme.example	203.0.113.10	External	recon	acme.example (resolves)	none	0	Known (4 runs)
host	admin.acme.example	203.0.113.11	External	recon	acme.example (resolves)	Critical	6	Known (4 runs)
host	api.acme.example	203.0.113.12	External	recon	acme.example (resolves)	none	0	Known (4 runs)
service	https/443 nginx	203.0.113.10:443	External	web	www.acme.example (hosts)	none	0	Known (18 runs)
service	https/443 tomcat	203.0.113.12:443	External	web	api.acme.example (hosts)	Critical	4	Known (18 runs)
service	postgresql/5432	203.0.113.12:5432	External	infra	api.acme.example (hosts)	none	0	Known (18 runs)
bucket	acme.example-assets	n/a	External	infra	acme.example (references)	High	1	Known (4 runs)
host	db-01.internal	10.20.0.5	Internal	infra	postgresql/5432 (connects)	none	0	Known (18 runs)

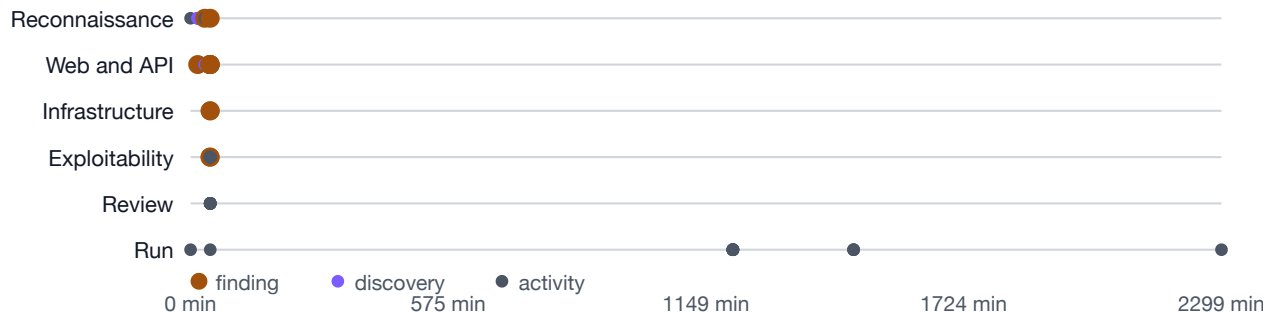
Discoveries

Live discoveries feed

When	Category	Label	Phase	Capability	Source
26 Sep 2026 17:28 UTC	subdomain	acme.example	recon	DNS intelligence	event
26 Sep 2026 17:28 UTC	subdomain	status.acme.example	recon	Open-source intel	event
26 Sep 2026 17:28 UTC	target	www.acme.example	recon	Open-source intel	event
26 Sep 2026 17:28 UTC	target	admin.acme.example	recon	DNS intelligence	event
26 Sep 2026 17:44 UTC	target	api.acme.example	recon	Open-source intel	event
26 Sep 2026 17:44 UTC	service	https/443 nginx	web	Dependency risk	event
26 Sep 2026 17:56 UTC	service	https/443 tomcat	web	Integration scanning	event
26 Sep 2026 17:56 UTC	service	postgresql/5432	infra	Dependency risk	event
26 Sep 2026 17:56 UTC	target	acme.example-assets	infra	Cloud posture	event
26 Sep 2026 17:56 UTC	target	db-01.internal	infra	Cloud posture	event

10. Attack narrative and kill chain

Assessment complete. Risk score 100.



Activity across the run: findings, discoveries and activity lines per phase.

Reconnaissance (ORION, Done, 31 min)

ORION completed the phase, recording 5 discoveries and 2 findings with DNS intelligence, Open-source intel, Vulnerability correlation. Last reasoning line: "Recorded DNS and TLS handshake observations for the public hosts".

- 26 Sep 2026 17:12 UTC Discovered domain acme.example
- 26 Sep 2026 17:12 UTC Discovered dns status.acme.example
- 26 Sep 2026 17:12 UTC Discovered host www.acme.example
- 26 Sep 2026 17:13 UTC Discovered host admin.acme.example
- 26 Sep 2026 17:13 UTC Discovered host api.acme.example
- F-08 Database port reachable from the internet **High**
- F-06 Dangling DNS record allows subdomain takeover **High**

Web and API Security (VEGA, Done, 12 min)

VEGA completed the phase, recording 2 discoveries and 6 findings with Integration scanning, Dependency risk, Source-code review, Browser attack paths. Last reasoning line: "Cross-referencing framework versions against the advisory feed".

- 26 Sep 2026 17:13 UTC Discovered service https/443 nginx
- 26 Sep 2026 17:13 UTC Discovered service https/443 tomcat
- F-12 Directory listing enabled **Low**
- F-02 SQL injection in search parameter **Critical**
- F-10 Login portal does not enforce multi-factor authentication **Medium**
- F-11 Security headers missing (CSP, HSTS) **Low**
- F-04 Default credentials accepted on management service **High**
- F-05 Source control metadata exposed (.git directory) **High**

Infrastructure and Configuration (ATLAS, Done, 11 s)

ATLAS completed the phase, recording 3 discoveries and 2 findings with Dependency risk, Cloud posture, Vulnerability correlation, DNS intelligence. Last reasoning line: "Correlating infra results against 10 assets".

- 26 Sep 2026 17:13 UTC Discovered service postgresql/5432
- 26 Sep 2026 17:13 UTC Discovered bucket acme.example-assets

- 26 Sep 2026 17:13 UTC Discovered host db-01.internal
- **F-09** Outdated TLS protocol versions accepted **Medium**
- **F-07** Publicly listable cloud storage bucket **High**

Exploitability Validation (NOVA, Done, 11 s)

NOVA completed the phase, recording 0 discoveries and 2 findings with Offensive toolchain, Browser attack paths, Vulnerability correlation, Hidden-data inspection, Remote-asset exposure. Last reasoning line: "Correlating exploit results against 10 assets".

- **F-01** Backdoored xz/liblzma package installed **Critical**
- **F-03** Apache HTTP Server path traversal **High**

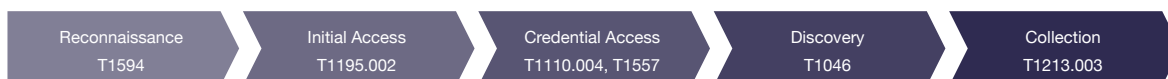
Review and Reporting (POLARIS, Done, 9 s)

POLARIS completed the phase, recording 0 discoveries and 0 findings. Last reasoning line: "Correlating review results against 10 assets".

Derived attack paths

admin.acme.example to admin.acme.example **Critical**

Critical path from the externally reachable host admin.acme.example; 6 findings enable Reconnaissance, Initial Access, Credential Access, Discovery, Collection.



Tactic sequence of admin.acme.example to admin.acme.example.

Assets: admin.acme.example (external). Findings: **F-01**, **F-05**, **F-08**, **F-10**, **F-11**, **F-12**.

https/443 tomcat to https/443 tomcat **Critical**

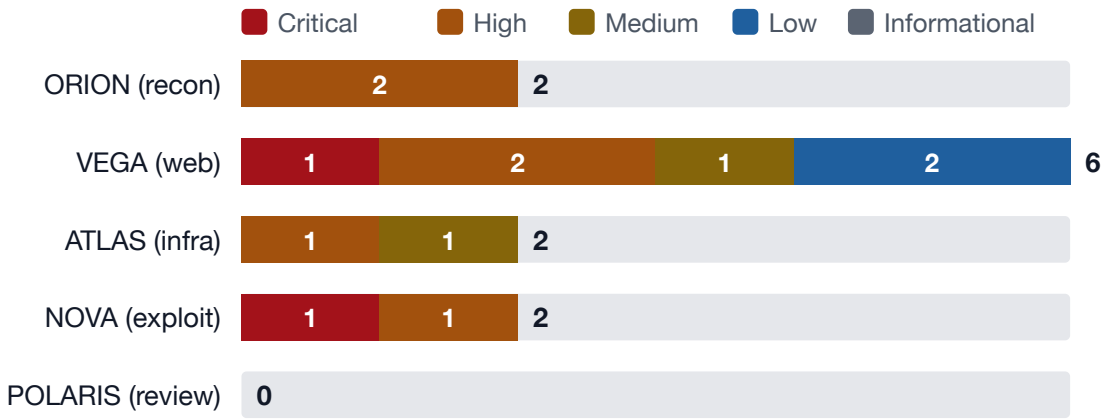
Critical path from the externally reachable service https/443 tomcat; 4 findings enable Initial Access, Credential Access.



Tactic sequence of https/443 tomcat to https/443 tomcat.

Assets: https/443 tomcat (external). Findings: **F-02**, **F-03**, **F-04**, **F-09**.

Severity by phase



Findings raised in each phase by severity.

11. Vulnerability intelligence

2

Distinct CVEs

2

Findings with CVEs

2

Critical or high

n/a

EPSS at or above 0.10
EPSS not fetched



Referenced CVEs

CVE	Worst	Findings	Assets	CVSS	EPSS	Recent feed	Last seen
CVE-2024-3094	Critical	F-01	1	10	not scored	no	26 Sep 2026 17:56 UTC
CVE-2021-41773	High	F-03	1	7.5	not scored	no	30 Sep 2026 02:00 UTC

CVE detail

CVE-2024-3094 Critical

Malicious code was discovered in the upstream tarballs of xz, starting with version 5.6.0, that modifies liblzma and can be used to intercept and modify data interaction with the library.

Published 29 Mar 2024 17:15 UTC; modified 6 Feb 2025 09:15 UTC; CVSS 10 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H); CWE-506.

- <https://nvd.nist.gov/vuln/detail/CVE-2024-3094>

CVE-2021-41773 High

A flaw was found in a change made to path normalization in Apache HTTP Server 2.4.49. An attacker could use a path traversal attack to map URLs to files outside the directories configured by Alias-like directives.

Published 5 Oct 2021 09:15 UTC; modified 29 Jan 2025 17:15 UTC; CVSS 7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N); CWE-22.

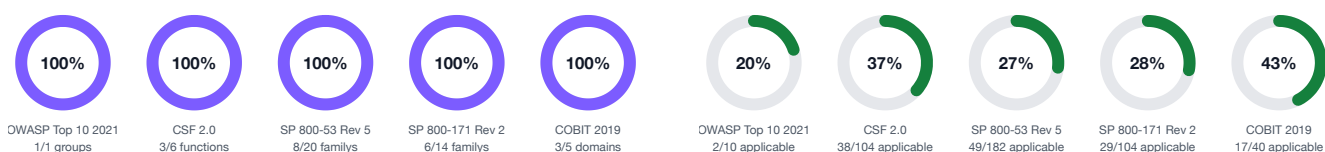
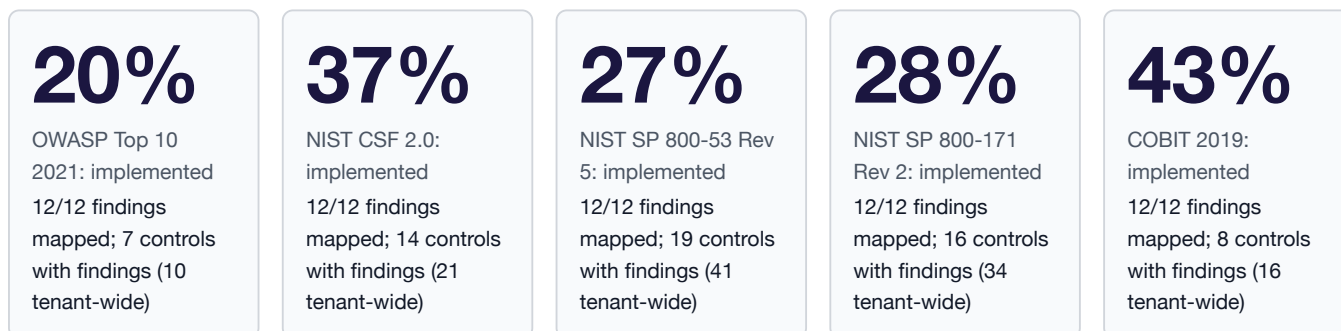
- <https://nvd.nist.gov/vuln/detail/CVE-2021-41773>
- https://httpd.apache.org/security/vulnerabilities_24.html

Weakness classes (CWE)

CWE	Findings	Refs
CWE-284	3	F-06 F-07 F-08
CWE-1021	1	F-11
CWE-1392	1	F-04

CWE	Findings	Refs
CWE-22	1	F-03
CWE-307	1	F-10
CWE-308	1	F-10
CWE-326	1	F-09
CWE-327	1	F-09
CWE-506	1	F-01
CWE-538	1	F-05

12. Compliance and control mapping

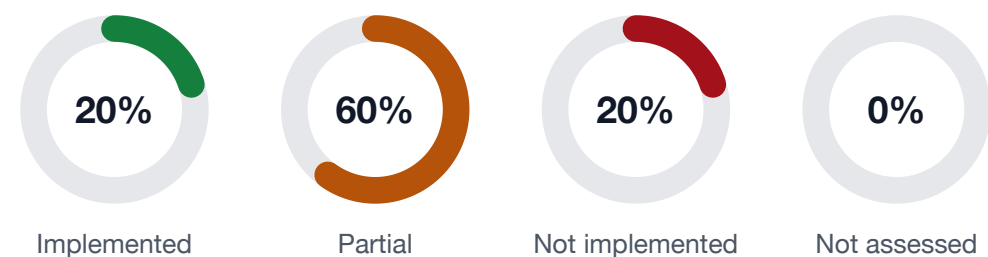
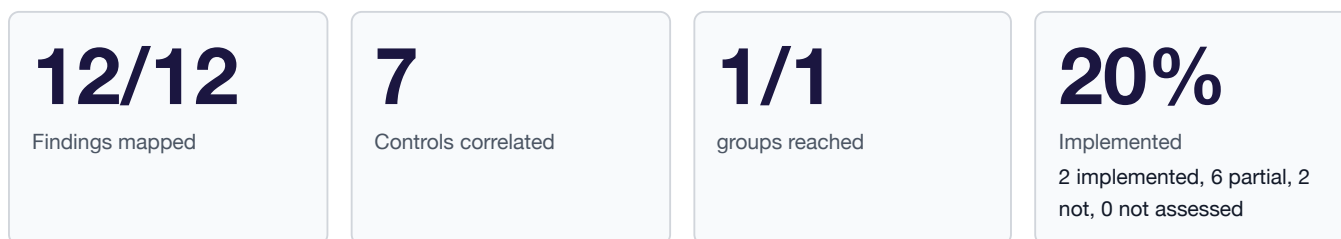


Share of findings mapped per framework, with the groups reached.

Implemented share of applicable controls (tenant-wide governance state).

Control status, owner, note and evidence are tenant-wide governance state shared by every assessment of the account, snapshotted when this issue was generated; only the mapped-findings figures are scoped to this assessment. 'Controls with findings' is given both for this run and tenant-wide, the latter being the number the console's compliance band prints.

OWASP Top 10 2021 (2021)



OWASP Top 10 2021: control status across 10 applicable controls.

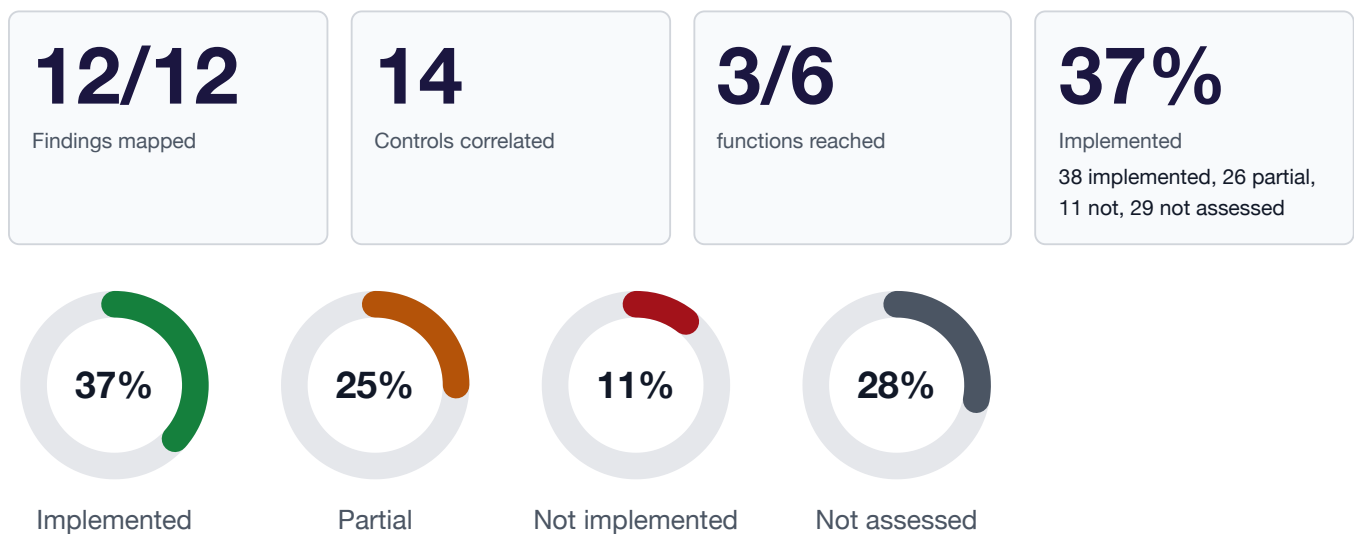
Controls with findings in this run

Control	Group	Findings	Worst	Refs	Status	Owner	Evidence
A01:2021 Broken Access Control	n/a	4 (4 open)	High	F-03 F-05 F-07 F-12	Partial	Application security	0

Control	Group	Findings	Worst	Refs	Status	Owner	Evidence
A02:2021 Cryptographic Failures	n/a	1 (1 open)	Medium	F-09	Partial	Platform team	1
A03:2021 Injection	n/a	1 (1 open)	Critical	F-02	Partial	Application security	0
A05:2021 Security Misconfiguration	n/a	7 (6 open)	High	F-04 F-05 F-06 F-07 F-08 F-11 F-12	Partial	Platform team	1
A06:2021 Vulnerable and Outdated Components	n/a	2 (2 open)	Critical	F-01 F-03	Partial	Platform team	1
A07:2021 Identification and Authentication Failures	n/a	2 (1 open)	High	F-04 F-10	Not implemented	Identity team	0
A08:2021 Software and Data Integrity Failures	n/a	1 (1 open)	Critical	F-01	Partial	Platform team	0

► 3 further assessed controls without findings

NIST CSF 2.0 (2.0)



NIST CSF 2.0: control status across 104 applicable controls.

Controls with findings in this run

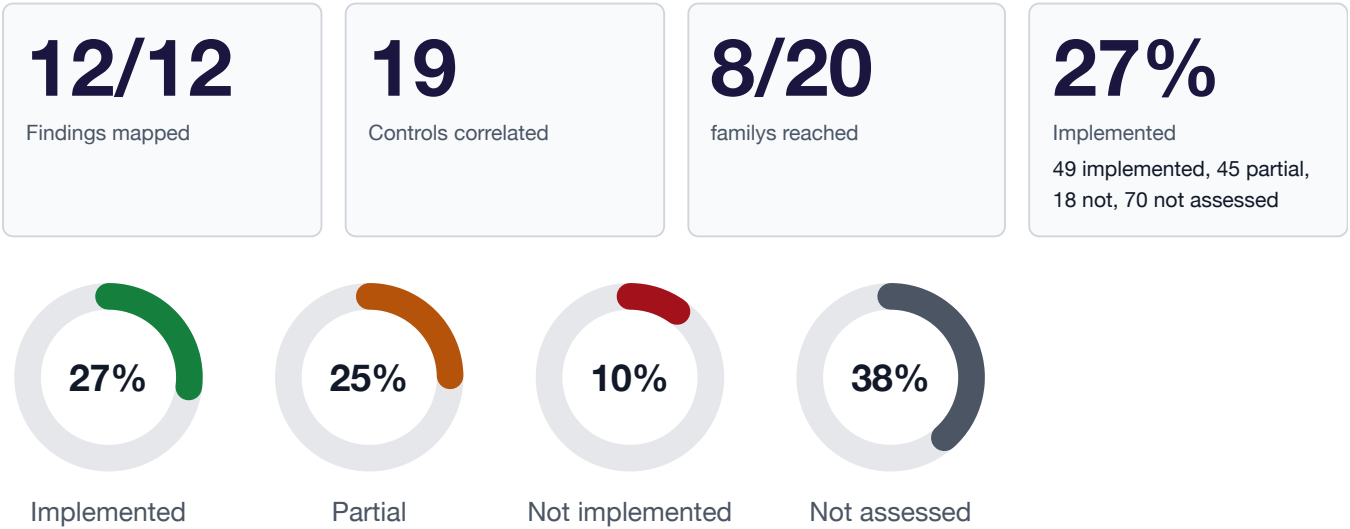
Control	Function	Findings	Worst	Refs	Status	Owner	Evidence
ID.AM-02 Inventories of software, services, and systems managed by the organization are maintained	Identify	1 (1 open)	High	F-06	Partial	Platform team	1

Control	Function	Findings	Worst	Refs	Status	Owner	Evidence
ID. AM-08 Systems, hardware, software, services, and data are managed throughout their life cycles	Identify	1 (1 open)	High	F-06	Partial	Security engineering	0
ID. RA-01 Vulnerabilities in assets are identified, validated, and recorded	Identify	2 (2 open)	Critical	F-02 F-03	✓ Implemented	Security engineering	0
ID. RA-09 The authenticity and integrity of hardware and software are assessed prior to acquisition and use	Identify	1 (1 open)	Critical	F-01	✗ Not implemented	Security engineering	0
PR. AA-01 Identities and credentials for authorized users, services, and hardware are managed by the organization	Protect	2 (1 open)	High	F-04 F-10	Partial	Identity team	0
PR. AA-03 Users, services, and hardware are authenticated	Protect	2 (1 open)	High	F-04 F-10	Partial	Identity team	1
PR. AA-05 Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties	Protect	1 (1 open)	High	F-07	Partial	Identity team	0
PR. DS-01 The confidentiality, integrity, and availability of data-at-rest are protected	Protect	1 (1 open)	High	F-07	Partial	Data protection officer	0
PR. DS-02 The confidentiality, integrity, and availability of data-in-transit are protected	Protect	1 (1 open)	Medium	F-09	Partial	Platform team	0
PR. PS-01 Configuration management practices are established and applied	Protect	4 (3 open)	High	F-04 F-05 F-11 F-12	Partial	Platform team	0
PR. PS-02 Software is maintained, replaced, and removed commensurate with risk	Protect	2 (2 open)	Critical	F-01 F-03	Partial	Platform team	0
PR. PS-06 Secure software development practices are integrated, and their performance is monitored throughout the software development life cycle	Protect	2 (2 open)	Critical	F-02 F-05	Partial	Platform team	0

Control	Function	Findings	Worst	Refs	Status	Owner	Evidence
PR. IR-01 Networks and environments are protected from unauthorized logical access and usage	Protect	1 (1 open)	High	F-08	Partial	Network team	0
DE. CM-01 Networks and network services are monitored to find potentially adverse events	Detect	1 (1 open)	High	F-08	Implemented	Security operations	1

► 63 further assessed controls without findings

NIST SP 800-53 Rev 5 (5.1.1)



NIST SP 800-53 Rev 5: control status across 182 applicable controls.

Controls with findings in this run

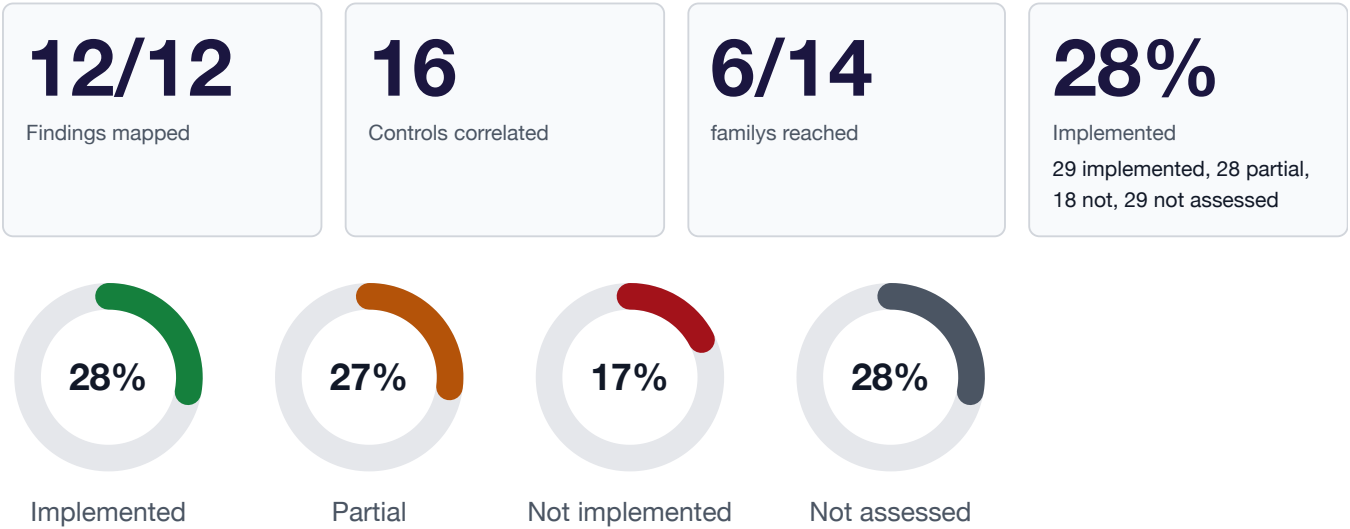
Control	Family	Findings	Worst	Refs	Status	Owner	Evidence
AC-3 Access Enforcement	Access Control	1 (1 open)	High	F-07	Partial	Application security	0
AC-6 Least Privilege	Access Control	1 (1 open)	High	F-07	Partial	Identity team	0
AC-7 Unsuccessful Logon Attempts	Access Control	1 (1 open)	Medium	F-10	Not implemented	Identity team	0
AC-22 Publicly Accessible Content	Access Control	1 (1 open)	High	F-07	Not implemented	Identity team	0
CM-6 Configuration Settings	Configuration Management	5 (4 open)	High	F-04 F-05 F-06 F-11 F-12	Partial	Platform team	0

Control	Family	Findings	Worst	Refs	Status	Owner	Evidence
CM-7 Least Functionality	Configuration Management	3 (3 open)	High	F-05 F-08 F-12	Partial	Platform team	0
CM-8 System Component Inventory	Configuration Management	1 (1 open)	High	F-06	Partial	IT operations	0
IA-2 Identification and Authentication (Organizational Users)	Identification and Authentication	2 (1 open)	High	F-04 F-10	Partial	Identity team	0
IA-5 Authenticator Management	Identification and Authentication	1 (0 open)	High	F-04	Partial	Identity team	0
RA-5 Vulnerability Monitoring and Scanning	Risk Assessment	1 (1 open)	High	F-03	✓ Implemented	Security engineering	1
SA-11 Developer Testing and Evaluation	System and Services Acquisition	1 (1 open)	Critical	F-02	Partial	Procurement	0
SC-7 Boundary Protection	System and Communications Protection	1 (1 open)	High	F-08	Partial	Network team	1
SC-8 Transmission Confidentiality and Integrity	System and Communications Protection	2 (2 open)	Medium	F-09 F-11	Partial	Platform team	0
SC-13 Cryptographic Protection	System and Communications Protection	1 (1 open)	Medium	F-09	✓ Implemented	Security engineering	0
SI-2 Flaw Remediation	System and Information Integrity	2 (2 open)	Critical	F-01 F-03	Partial	Platform team	0
SI-7 Software, Firmware, and Information Integrity	System and Information Integrity	1 (1 open)	Critical	F-01	✗ Not implemented	Platform team	0
SI-10 Information Input Validation	System and Information Integrity	2 (2 open)	Critical	F-02 F-03	Partial	Application security	0
SR-3 Supply Chain Controls and Processes	Supply Chain Risk Management	1 (1 open)	Critical	F-01	✗ Not implemented	Procurement	0

Control	Family	Findings	Worst	Refs	Status	Owner	Evidence
SR-11 Component Authenticity	Supply Chain Risk Management	1 (1 open)	Critical	F-01	Partial	Procurement	0

► 109 further assessed controls without findings

NIST SP 800-171 Rev 2 (r2)



NIST SP 800-171 Rev 2: control status across 104 applicable controls.

Controls with findings in this run

Control	Family	Findings	Worst	Refs	Status	Owner	Evidence
3.1.1 Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	Access Control	1 (1 open)	High	F-07	Partial	Identity team	0
3.1.8 Limit unsuccessful logon attempts.	Access Control	1 (1 open)	Medium	F-10	Not implemented	Identity team	0
3.1.22 Control CUI posted or processed on publicly accessible systems.	Access Control	1 (1 open)	High	F-07	Partial	Identity team	0

Control	Family	Findings	Worst	Refs	Status	Owner	Evidence
3.4.1 Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	Configuration Management	1 (1 open)	High	F-06	Partial	IT operations	0
3.4.2 Establish and enforce security configuration settings for information technology products employed in organizational systems.	Configuration Management	3 (2 open)	High	F-04 F-05 F-11	Partial	Platform team	0
3.4.6 Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	Configuration Management	1 (1 open)	Low	F-12	Not implemented	Platform team	0
3.4.7 Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.	Configuration Management	3 (3 open)	High	F-05 F-08 F-12	Partial	Platform team	0
3.5.2 Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems.	Identification and Authentication	1 (0 open)	High	F-04	Not assessed	n/a	0
3.5.3 Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.	Identification and Authentication	2 (1 open)	High	F-04 F-10	Partial	Identity team	1
3.11.3 Remediate vulnerabilities in accordance with risk assessments.	Risk Assessment	1 (1 open)	High	F-03	Partial	Security engineering	0

Control	Family	Findings	Worst	Refs	Status	Owner	Evidence
3.13.1 Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.	System and Communications Protection	1 (1 open)	High	F-08	Partial	Network team	0
3.13.2 Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	System and Communications Protection	1 (1 open)	Critical	F-02	Not implemented	Network team	0
3.13.5 Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	System and Communications Protection	1 (1 open)	High	F-08	Partial	Network team	0
3.13.8 Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.	System and Communications Protection	2 (2 open)	Medium	F-09 F-11	Partial	Platform team	1
3.14.1 Identify, report, and correct system flaws in a timely manner.	System and Information Integrity	3 (3 open)	Critical	F-01 F-02 F-03	Partial	Platform team	0
3.14.2 Provide protection from malicious code at designated locations within organizational systems.	System and Information Integrity	1 (1 open)	Critical	F-01	Not implemented	Platform team	0

► 66 further assessed controls without findings

COBIT 2019 (2019)**12/12**

Findings mapped

8

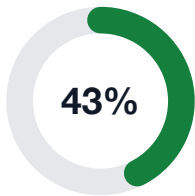
Controls correlated

3/5

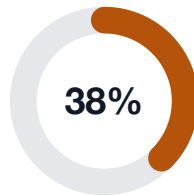
domains reached

43%

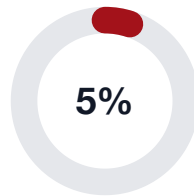
Implemented

17 implemented, 15 partial,
2 not, 6 not assessed

Implemented



Partial



Not implemented



Not assessed

COBIT 2019: control status across 40 applicable controls.

Controls with findings in this run

Control	Domain	Findings	Worst	Refs	Status	Owner	Evidence
AP010 Managed Vendors	Align, Plan and Organize	1 (1 open)	Critical	F-01	Partial	Procurement	0
AP012 Managed Risk	Align, Plan and Organize	2 (2 open)	Critical	F-01 F-03	Partial	GRC	1
AP013 Managed Security	Align, Plan and Organize	1 (0 open)	High	F-04	Implemented	CISO	2
AP014 Managed Data	Align, Plan and Organize	1 (1 open)	High	F-07	Not implemented	Data protection officer	0
BAI03 Managed Solutions Identification and Build	Build, Acquire and Implement	1 (1 open)	Critical	F-02	Partial	Engineering leadership	0
BAI09 Managed Assets	Build, Acquire and Implement	1 (1 open)	High	F-06	Partial	IT operations	0
BAI10 Managed Configuration	Build, Acquire and Implement	5 (5 open)	High	F-05 F-06 F-08 F-11 F-12	Partial	Platform team	0
DSS05 Managed Security Services	Deliver, Service and Support	8 (7 open)	Critical	F-02 F-03 F-04 F-05 F-07 F-08 F-09 F-10	Partial	Security operations	0

► 26 further assessed controls without findings

Crosswalk

Crosswalk: findings to controls

Ref	Finding	OWASP	NIST CSF	SP 800-53	SP 800-171	COBIT
F-01	Backdoored xz/liblzma package installed	A08:2021, A06:2021	ID.RA-09, PR.PS-02	SR-3, SR-11, SI-7, SI-2	3.14.1, 3.14.2	APO10, APO12
F-02	SQL injection in search parameter	A03:2021	PR.PS-06, ID.RA-01	SI-10, SA-11	3.14.1, 3.13.2	BAI03, DSS05
F-03	Apache HTTP Server path traversal	A01:2021, A06:2021	ID.RA-01, PR.PS-02	SI-2, SI-10, RA-5	3.14.1, 3.11.3	APO12, DSS05
F-04	Default credentials accepted on management service	A07:2021, A05:2021	PR.AA-01, PR.AA-03, PR.PS-01	IA-5, IA-2, CM-6	3.5.2, 3.5.3, 3.4.2	DSS05, APO13
F-05	Source control metadata exposed (.git directory)	A05:2021, A01:2021	PR.PS-01, PR.PS-06	CM-7, CM-6	3.4.2, 3.4.7	BAI10, DSS05
F-06	Dangling DNS record allows subdomain takeover	A05:2021	ID.AM-02, ID.AM-08	CM-8, CM-6	3.4.1	BAI09, BAI10
F-07	Publicly listable cloud storage bucket	A01:2021, A05:2021	PR.DS-01, PR.AA-05	AC-3, AC-6, AC-22	3.1.1, 3.1.22	DSS05, APO14
F-08	Database port reachable from the internet	A05:2021	PR.IR-01, DE.CM-01	SC-7, CM-7	3.13.1, 3.13.5, 3.4.7	DSS05, BAI10
F-09	Outdated TLS protocol versions accepted	A02:2021	PR.DS-02	SC-8, SC-13	3.13.8	DSS05
F-10	Login portal does not enforce multi-factor authentication	A07:2021	PR.AA-03, PR.AA-01	IA-2, AC-7	3.5.3, 3.1.8	DSS05
F-11	Security headers missing (CSP, HSTS)	A05:2021	PR.PS-01	CM-6, SC-8	3.4.2, 3.13.8	BAI10
F-12	Directory listing enabled	A05:2021, A01:2021	PR.PS-01	CM-7, CM-6	3.4.6, 3.4.7	BAI10

Evidence index

Framework	Control	File	Type	Bytes	Uploaded
OWASP Top 10 2021	A02:2021	tls-configuration-scan.txt	text/plain	511	22 Sep 2026 01:41 UTC
OWASP Top 10 2021	A04:2021	threat-model-register.csv	text/csv	394	17 Sep 2026 01:41 UTC
OWASP Top 10 2021	A05:2021	web-hardening-baseline.md	text/markdown	508	22 Sep 2026 14:01 UTC
OWASP Top 10 2021	A06:2021	dependency-inventory.csv	text/csv	271	19 Sep 2026 14:01 UTC
OWASP Top 10 2021	A09:2021	siem-alert-coverage.csv	text/csv	452	12 Sep 2026 01:41 UTC

Framework	Control	File	Type	Bytes	Uploaded
NIST CSF 2.0	GV.RR-02	security-raci.csv	text/csv	400	7 Sep 2026 01:41 UTC
NIST CSF 2.0	GV.PO-01	information-security-policy-approval.pdf	application/pdf	1101	13 Aug 2026 01:41 UTC
NIST CSF 2.0	GV.PO-01	information-security-policy-excerpt.md	text/markdown	429	22 Sep 2026 14:01 UTC
NIST CSF 2.0	ID.AM-02	external-asset-inventory.csv	text/csv	324	19 Sep 2026 14:01 UTC
NIST CSF 2.0	PR.AA-03	sso-mfa-enforcement.png	image/png	1826	18 Aug 2026 01:41 UTC
NIST CSF 2.0	PR.AT-01	awareness-training-completion.csv	text/csv	244	2 Sep 2026 01:41 UTC
NIST CSF 2.0	PR.DS-11	backup-restore-test-2026-09.md	text/markdown	657	28 Aug 2026 01:41 UTC
NIST CSF 2.0	DE.CM-01	monitoring-coverage.txt	text/plain	241	16 Sep 2026 14:01 UTC
NIST CSF 2.0	RS.MA-01	tabletop-exercise-summary.md	text/markdown	589	23 Aug 2026 01:41 UTC
NIST SP 800-53 Rev 5	AC-2	access-review-2026-q3.csv	text/csv	283	8 Aug 2026 01:41 UTC
NIST SP 800-53 Rev 5	AU-2	logging-standard-excerpt.md	text/markdown	462	22 Sep 2026 01:41 UTC
NIST SP 800-53 Rev 5	CM-2	baseline-images.csv	text/csv	245	17 Sep 2026 01:41 UTC
NIST SP 800-53 Rev 5	CP-9	backup-restore-test-2026-09.md	text/markdown	657	12 Sep 2026 01:41 UTC
NIST SP 800-53 Rev 5	IR-8	incident-response-plan-excerpt.md	text/markdown	476	19 Sep 2026 14:01 UTC
NIST SP 800-53 Rev 5	RA-5	vulnerability-scan-schedule.csv	text/csv	318	22 Sep 2026 14:01 UTC
NIST SP 800-53 Rev 5	SC-7	waf-dashboard.png	image/png	1731	7 Sep 2026 01:41 UTC
NIST SP 800-171 Rev 2	3.1.12	vpn-session-logging.txt	text/plain	338	18 Aug 2026 01:41 UTC
NIST SP 800-171 Rev 2	3.3.1	log-retention-policy.md	text/markdown	305	2 Sep 2026 01:41 UTC
NIST SP 800-171 Rev 2	3.5.3	mfa-enrolment-report.csv	text/csv	174	22 Sep 2026 14:01 UTC
NIST SP 800-171 Rev 2	3.6.1	incident-exercise-log.csv	text/csv	247	28 Aug 2026 01:41 UTC

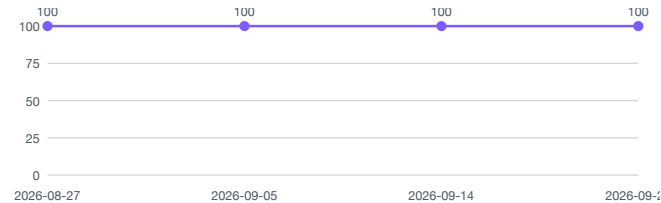
Framework	Control	File	Type	Bytes	Uploaded
NIST SP 800-171 Rev 2	3.11.2	vulnerability-scan-schedule.csv	text/csv	318	23 Aug 2026 01:41 UTC
NIST SP 800-171 Rev 2	3.13.8	encryption-in-transit-standard.md	text/markdown	348	19 Sep 2026 14:01 UTC
COBIT 2019	EDM03	risk-committee-minutes-excerpt.md	text/markdown	424	13 Aug 2026 01:41 UTC
COBIT 2019	APO12	risk-register-extract.csv	text/csv	436	22 Sep 2026 14:01 UTC
COBIT 2019	APO13	iso27001-certificate.pdf	application/pdf	1213	17 Sep 2026 01:41 UTC
COBIT 2019	APO13	isms-scope-statement.md	text/markdown	312	19 Sep 2026 14:01 UTC
COBIT 2019	DSS04	dr-test-report-2026.md	text/markdown	378	8 Aug 2026 01:41 UTC
COBIT 2019	MEA01	security-kpi-dashboard-2026-08.csv	text/csv	283	22 Sep 2026 01:41 UTC

Not covered by this gateway: masvs (mobile_app), cis-aws (cloud_account), cis-azure (cloud_account), cis-gcp (cloud_account), cis_m365 (ms_tenant), scuba (ms_tenant).

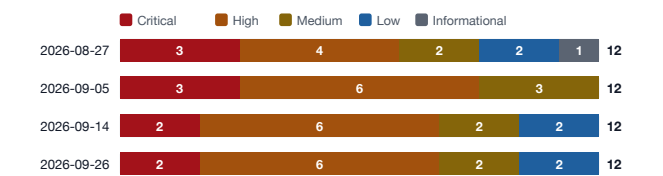
13. Assessment history and trend

Runs of this target

Run	Profile	Status	Created	Finished	Risk	Findings	Depth
scn_22f52748d76148de	deep	Completed	27 Aug 2026 14:03 UTC	27 Aug 2026 14:48 UTC	100	12	0
scn_30c8594ccd5e4867	deep	Completed	5 Sep 2026 14:03 UTC	5 Sep 2026 14:48 UTC	100	12	1
scn_19396660eb634c82	deep	Completed	14 Sep 2026 14:03 UTC	14 Sep 2026 14:48 UTC	100	12	2
scn_cb416011e91841c3 (this issue)	deep	Completed	26 Sep 2026 17:12 UTC	26 Sep 2026 17:56 UTC	100	12	3



Risk score across completed runs.



Findings per run by severity.

Change against the parent run

0

New findings

0

Resolved since parent

12

Persisting

0

Net change
parent
scn_19396660eb634c82

New in this run

None.

Resolved since the parent run

None.

Persisting

Finding	Severity
F-01 Backdoored xz/liblzma package installed	Critical
F-02 SQL injection in search parameter	Critical
F-03 Apache HTTP Server path traversal	High
F-04 Default credentials accepted on management service	High
F-05 Source control metadata exposed (.git directory)	High

Finding	Severity
F-06 Dangling DNS record allows subdomain takeover	High
F-07 Publicly listable cloud storage bucket	High
F-08 Database port reachable from the internet	High
F-09 Outdated TLS protocol versions accepted	Medium
F-10 Login portal does not enforce multi-factor authentication	Medium
F-11 Security headers missing (CSP, HSTS)	Low
F-12 Directory listing enabled	Low

Schedules

Schedules

Cadence	Profile	Enabled	Last run	Next run
weekly	deep	yes	26 Sep 2026 17:12 UTC	3 Oct 2026 17:03 UTC

14. Conclusion and next steps

The deep assessment of acme.example completed on 26 September 2026 with a risk score of 100 (Critical), unchanged from the previous run. 12 findings were observed across 10 assets: 2 critical, 6 high, 2 medium, 2 low. By status: 11 open, 1 marked as a false positive.

Overall posture: **Critical** (score 100); 11 of 12 findings remain open.

Top three actions

1. **F-01** Backdoored xz/liblzma package installed: Downgrade xz-utils to 5.4.x and rebuild affected hosts from a clean image.
2. **F-02** SQL injection in search parameter: Use parameterised queries and least-privilege database credentials.
3. **F-08** Database port reachable from the internet: Bind the database to private interfaces and restrict with security groups.

Retest: a weekly schedule is in place, next run 3 Oct 2026 17:03 UTC. Resolved findings are only closed when a later run no longer observes them.

Prepared by Sam Rivera, Lead Security Consultant (fictional), on 29 September 2026.

Appendix A Agents, capabilities and datasets



Share of declared capabilities each agent exercised in this run.

Agent roster

Agent	Phase	Role	Declared capabilities	Exercised	Findings	Status
ORION	recon	Maps the public attack surface	Open-source intel, DNS intelligence, Vulnerability correlation, Source-code review	DNS intelligence, Open-source intel, Vulnerability correlation	2	done
VEGA	web	Probes web and API input handling, sessions, and headers	Source-code review, Dependency risk, Integration scanning	Integration scanning, Dependency risk, Source-code review	6	done
ATLAS	infra	Assesses cloud, transport, and the internal segment	Cloud posture, DNS intelligence, Dependency risk, Vulnerability correlation	Dependency risk, Cloud posture, Vulnerability correlation, DNS intelligence	2	done
NOVA	exploit	Validates exploitability to benign proof	Offensive toolchain, Vulnerability correlation, Browser attack paths, Breach exposure, Hidden-data inspection, Remote-asset exposure	Offensive toolchain, Browser attack paths, Vulnerability correlation, Hidden-data inspection, Remote-asset exposure	2	done
POLARIS	review	Consolidates findings and maps them to control frameworks	none (synthesis)	none	0	done
SCRIBE	n/a	Writes the client-deliverable report	none (synthesis)	none	0	done

Datasets

Dataset	Version	Source
MITRE ATT&CK Enterprise	v15.1	gateway/src/catalogs/attack.js
OWASP Top 10 2021	2021	gateway/src/catalogs/owasp.js

Dataset	Version	Source
NIST CSF 2.0	2.0	gateway/src/catalogs/nistcsf.js
NIST SP 800-53 Rev 5	5.1.1	gateway/src/catalogs/nist80053.js
NIST SP 800-171 Rev 2	r2	gateway/src/catalogs/nist800171.js
COBIT 2019	2019	gateway/src/catalogs/cobit.js
NVD CVE records	2026-09-30T05:45:50.246Z	gateway cve_cache / cve_feed

Feeds

NVD feed last refreshed

30 Sep 2026 05:45 UTC

EPSS

not fetched

Collectors

Name	Status	Authorised scopes	Internal scans	Last seen
Legacy VPN probe	revoked	10.99.0.0/16	authorised	26 Aug 2026 01:41 UTC
Frankfurt data centre sensor	active	10.20.0.0/16, 172.16.8.0/22	authorised	25 Sep 2026 01:38 UTC
Amsterdam office sensor	active	10.10.0.0/16	authorised	23 Sep 2026 16:58 UTC
Singapore office sensor	pending	192.168.40.0/24	not authorised	
Contoso DC collector	active	ad:forest:corp.example.com	authorised	27 Sep 2026 16:27 UTC

Appendix B Severity, risk and CVSS definitions

Severity

Severity	CVSS band	Definition
Critical	9.0 to 10.0	Exploitable without preconditions, with a direct path to full compromise of the affected system or data.
High	7.0 to 8.9	Significant impact with realistic exploitation, or a weakness that materially shortens an attacker's path.
Medium	4.0 to 6.9	Moderate impact, or exploitation depends on preconditions such as user interaction or an existing foothold.
Low	0.1 to 3.9	Limited impact on its own; typically hardening or hygiene.
Informational	0.0	An observation without direct security impact, recorded for completeness.

Risk score = $\min(100, \text{critical} \times 25 + \text{high} \times 12 + \text{medium} \times 5 + \text{low} \times 2 + \text{info} \times 0)$ over every finding observed in the run, frozen when the run finished and not recomputed after triage. The open-only score applies the same formula to findings still open.

Risk bands

Band	Range
low	0 to 24
moderate	25 to 49
elevated	50 to 74
critical	75 to 100

Risk contributions in this run (scored; raw total 136, capped at 100)

Severity	Count	Weight	Points
Critical	2	25	50
High	6	12	72
Medium	2	5	10
Low	2	2	4
Informational	0	0	0

CVSS v3.1 base metrics

Metric	Description	Values
Attack Vector (AV)	How remote an attacker can be to exploit the weakness.	N = Network, A = Adjacent, L = Local, P = Physical
Attack Complexity (AC)	Conditions beyond the attacker's control that must exist.	L = Low, H = High

Metric	Description	Values
Privileges Required (PR)	The level of privilege the attacker needs beforehand.	N = None, L = Low, H = High
User Interaction (UI)	Whether a user other than the attacker must take part.	N = None, R = Required
Scope (S)	Whether the impact reaches beyond the vulnerable component.	U = Unchanged, C = Changed
Confidentiality (C)	Impact on the confidentiality of information.	N = None, L = Low, H = High
Integrity (I)	Impact on the trustworthiness of information.	N = None, L = Low, H = High
Availability (A)	Impact on the availability of the component.	N = None, L = Low, H = High

Confidence

Confidence	Definition
high	Confirmed by benign proof: a marker echo, a version readout or a configuration value observed directly.
medium	Consistent with the advisory or the observed behaviour, but exploitation depends on the deployment shape.
low	Inferred from indirect signals; verification is recommended before remediation is scheduled.

Status

Status	Definition
Open	Reported and not yet addressed.
In remediation	A fix is in progress; the finding remains counted until a retest confirms it.
Accepted risk	The owner has accepted the risk, with a reason and, where set, an expiry date for the exception.
Resolved	Closed; a rescan or retest no longer observes the condition.
False positive	Reviewed and judged not to be a real weakness.

Appendix C Glossary

Term	Definition
ATT&CK	MITRE's knowledge base of adversary tactics and techniques, used here to place each finding on the attacker's path.
Attack surface	Every asset the assessment could reach or infer: domains, records, hosts, services, storage and the internal hosts they connect to.
Benign proof	A probe that demonstrates a condition without exploiting it: a harmless plain-text marker, a read-only request, a version or configuration readout.
Control	A requirement in a compliance framework (OWASP Top 10, NIST CSF, SP 800-53, SP 800-171, COBIT) that a finding maps to.
CVE	A published identifier for a known vulnerability in a product or component, with its NVD record where the gateway holds one.
CVSS	The Common Vulnerability Scoring System; the base score and vector describe intrinsic severity and are informative here.
CWE	A catalogue entry describing the class of weakness behind a finding.
EPSS	FIRST's Exploit Prediction Scoring System; the probability of exploitation in the next 30 days when it has been fetched.
Exposure	Whether an asset is reachable from the internet (external) or only from inside the assessed network (internal).
Finding	One weakness on one asset, deduplicated across runs: a later run that sees it again adds an observation rather than a duplicate.
KEV	CISA's Known Exploited Vulnerabilities catalogue; a listed CVE is exploited in the wild.
Kill chain	A derived attack path: an external entry asset, the assets reachable from it and the ATT&CK tactics the findings along it enable.
Lineage	The runs of the same target in order, each linked to the run it repeated, so findings can be compared run to run.
Observation	The evidence one run recorded for a finding in one phase.
Phase	One stage of the assessment pipeline, owned by one agent.
Profile	The intensity of the run: recon (passive mapping), standard, or deep (adds exploitability validation).
Risk score	A 0 to 100 figure derived from the severities observed in the run, frozen when the run completed.
Retest	A later run of the same target that checks whether remediated findings are still observed.

Appendix D Evidence index and activity log

Evidence index

F-01 Backdoored xz/liblzma package installed exploit, 26 Sep 2026 17:56 UTC

```
banner: SSH-2.0-OpenSSH_9.6p1 Debian-4
package: xz-utils 5.6.1-1
```

F-02 SQL injection in search parameter web, 26 Sep 2026 17:56 UTC

```
notes: Error-based confirmation only; no timing or data-extraction probe was run.
request: GET /search?q=AQIRA-MARKER-sqli'
response: HTTP 500 - SQLSTATE 42601 syntax error near AQIRA-MARKER-sqli
```

F-03 Apache HTTP Server path traversal exploit, 26 Sep 2026 17:56 UTC

```
request: GET /cgi-bin/.%2e/AQIRA-MARKER-traversal.txt
version: Server: Apache/2.4.49 (Unix)
response: HTTP 200 - path normalisation escaped the CGI root; body contains AQIRA-MARKER-traversal
```

F-04 Default credentials accepted on management service web, 26 Sep 2026 17:56 UTC

```
login: admin / **** -> HTTP 200, session issued
service: management console
```

F-05 Source control metadata exposed (.git directory) web, 26 Sep 2026 17:56 UTC

```
url: https://acme.example/.git/HEAD
body: ref: refs/heads/main
```

F-05 Source control metadata exposed (.git directory) web, 26 Sep 2026 17:56 UTC

```
url: https://acme.example/.git/HEAD
body: ref: refs/heads/main
```

F-06 Dangling DNS record allows subdomain takeover recon, 26 Sep 2026 17:56 UTC

```
record: status.acme.example CNAME unclaimed-app.paas.example
response: The target responds: no such application
```

F-07 Publicly listable cloud storage bucket infra, 26 Sep 2026 17:56 UTC

```
url: https://acme.example-assets.storage.example/?list-type=2
objects: 1834
```

F-08 Database port reachable from the internet recon, 26 Sep 2026 17:44 UTC

port: 5432/tcp open
banner: PostgreSQL 13.4

F-09 Outdated TLS protocol versions accepted infra, 26 Sep 2026 17:56 UTC

cipher: TLS_RSA_WITH_AES_128_CBC_SHA
protocols: TLSv1.0, TLSv1.1, TLSv1.2

F-10 Login portal does not enforce multi-factor authentication web, 26 Sep 2026 17:56 UTC

attempts: Repeated failed sign-ins with no lockout or challenge

F-11 Security headers missing (CSP, HSTS) web, 26 Sep 2026 17:56 UTC

missing: content-security-policy, strict-transport-security

F-12 Directory listing enabled web, 26 Sep 2026 17:28 UTC

url: https://acme.example/uploads/
title: Index of /uploads

Activity log

Activity log (101 of 101 events)

#	When	Type	Category	Phase	Summary	Capability
1	26 Sep 2026 17:12 UTC	status	status	n/a	Assessment started (running, 1%)	n/a
2	26 Sep 2026 17:12 UTC	phase	phase	recon	Reconnaissance started (running)	n/a
3	26 Sep 2026 17:12 UTC	discovery	subdomain	recon	Discovered domain acme.example	DNS intelligence
4	26 Sep 2026 17:12 UTC	progress	status	recon	progress (running, 4%)	n/a
5	26 Sep 2026 17:12 UTC	discovery	subdomain	recon	Discovered dns status.acme.example	Open-source intel
6	26 Sep 2026 17:12 UTC	progress	status	recon	progress (running, 7%)	n/a
7	26 Sep 2026 17:12 UTC	discovery	target	recon	Discovered host www.acme.example	Open-source intel

#	When	Type	Category	Phase	Summary	Capability
8	26 Sep 2026 17:12 UTC	finding	finding	web	Directory listing enabled	Integration scanning
9	26 Sep 2026 17:12 UTC	progress	status	recon	progress (running, 10%)	n/a
10	26 Sep 2026 17:13 UTC	discovery	target	recon	Discovered host admin.acme.example	DNS intelligence
11	26 Sep 2026 17:13 UTC	progress	status	recon	progress (running, 13%)	n/a
12	26 Sep 2026 17:13 UTC	discovery	target	recon	Discovered host api.acme.example	Open-source intel
13	26 Sep 2026 17:13 UTC	progress	status	recon	progress (running, 16%)	n/a
14	26 Sep 2026 17:13 UTC	thinking	evidence	recon	Recorded DNS and TLS handshake observations for the public hosts	Vulnerability correlation
15	26 Sep 2026 17:13 UTC	finding	finding	recon	Database port reachable from the internet	DNS intelligence
16	26 Sep 2026 17:13 UTC	progress	status	recon	progress (running, 19%)	n/a
17	26 Sep 2026 17:13 UTC	phase	phase	recon	Reconnaissance complete (completed)	n/a
18	26 Sep 2026 17:13 UTC	phase	phase	web	Web and API Security started (running)	n/a
19	26 Sep 2026 17:13 UTC	discovery	service	web	Discovered service https/443 nginx	Dependency risk
20	26 Sep 2026 17:13 UTC	progress	status	web	progress (running, 22%)	n/a
21	26 Sep 2026 17:13 UTC	discovery	service	web	Discovered service https/443 tomcat	Integration scanning
22	26 Sep 2026 17:13 UTC	finding	finding	web	SQL injection in search parameter	Integration scanning

#	When	Type	Category	Phase	Summary	Capability
23	26 Sep 2026 17:13 UTC	progress	status	web	progress (running, 25%)	n/a
24	26 Sep 2026 17:13 UTC	thinking	analysis	web	Correlating web results against 7 assets	Source-code review
25	26 Sep 2026 17:13 UTC	progress	status	web	progress (running, 28%)	n/a
26	26 Sep 2026 17:13 UTC	thinking	validation	web	Reflected marker AQIRA-MARKER-web observed on /search; recorded as evidence, not exploited	Browser attack paths
27	26 Sep 2026 17:13 UTC	progress	status	web	progress (running, 31%)	n/a
28	26 Sep 2026 17:13 UTC	thinking	analysis	web	Correlating web results against 7 assets	Integration scanning
29	26 Sep 2026 17:13 UTC	finding	finding	web	Login portal does not enforce multi-factor authentication	Integration scanning
30	26 Sep 2026 17:13 UTC	progress	status	web	progress (running, 34%)	n/a
31	26 Sep 2026 17:13 UTC	thinking	analysis	web	Cross-referencing framework versions against the advisory feed	Dependency risk
32	26 Sep 2026 17:13 UTC	progress	status	web	progress (running, 37%)	n/a
33	26 Sep 2026 17:13 UTC	phase	phase	web	Web and API Security complete (completed)	n/a
34	26 Sep 2026 17:13 UTC	phase	phase	infra	Infrastructure and Configuration started (running)	n/a
35	26 Sep 2026 17:13 UTC	discovery	service	infra	Discovered service postgresql/5432	Dependency risk
36	26 Sep 2026 17:13 UTC	progress	status	infra	progress (running, 40%)	n/a
37	26 Sep 2026 17:13 UTC	discovery	target	infra	Discovered bucket acme.example-assets	Cloud posture

#	When	Type	Category	Phase	Summary	Capability
38	26 Sep 2026 17:13 UTC	finding	finding	web	Security headers missing (CSP, HSTS)	Integration scanning
39	26 Sep 2026 17:13 UTC	progress	status	infra	progress (running, 43%)	n/a
40	26 Sep 2026 17:13 UTC	discovery	target	infra	Discovered host db-01.internal	Cloud posture
41	26 Sep 2026 17:13 UTC	progress	status	infra	progress (running, 46%)	n/a
42	26 Sep 2026 17:13 UTC	thinking	analysis	infra	Correlating infra results against 10 assets	Cloud posture
43	26 Sep 2026 17:13 UTC	progress	status	infra	progress (running, 49%)	n/a
44	26 Sep 2026 17:13 UTC	thinking	evidence	infra	Bucket listing response captured for acme.example-assets (object count only)	Cloud posture
45	26 Sep 2026 17:13 UTC	finding	finding	exploit	Backdoored xz/liblzma package installed	Offensive toolchain
46	26 Sep 2026 17:13 UTC	progress	status	infra	progress (running, 52%)	n/a
47	26 Sep 2026 17:56 UTC	thinking	analysis	infra	Correlating infra results against 10 assets	Dependency risk
48	26 Sep 2026 17:56 UTC	progress	status	infra	progress (running, 55%)	n/a
49	26 Sep 2026 17:56 UTC	thinking	analysis	infra	Correlating infra results against 10 assets	Vulnerability correlation
50	26 Sep 2026 17:56 UTC	progress	status	infra	progress (running, 58%)	n/a
51	26 Sep 2026 17:56 UTC	phase	phase	infra	Infrastructure and Configuration complete (completed)	n/a
52	26 Sep 2026 17:56 UTC	phase	phase	exploit	Exploitability Validation started (running)	n/a

#	When	Type	Category	Phase	Summary	Capability
53	26 Sep 2026 17:56 UTC	thinking	analysis	exploit	Correlating exploit results against 10 assets	Browser attack paths
54	26 Sep 2026 17:56 UTC	finding	finding	exploit	Apache HTTP Server path traversal	Vulnerability correlation
55	26 Sep 2026 17:56 UTC	progress	status	exploit	progress (running, 61%)	n/a
56	26 Sep 2026 17:56 UTC	thinking	planning	exploit	Validating exploitability with benign probes; no state-changing requests	Offensive toolchain
57	26 Sep 2026 17:56 UTC	progress	status	exploit	progress (running, 64%)	n/a
58	26 Sep 2026 17:56 UTC	thinking	analysis	exploit	Correlating exploit results against 10 assets	Hidden-data inspection
59	26 Sep 2026 17:56 UTC	finding	finding	web	Default credentials accepted on management service	Integration scanning
60	26 Sep 2026 17:56 UTC	progress	status	exploit	progress (running, 67%)	n/a
61	26 Sep 2026 17:56 UTC	thinking	analysis	exploit	Correlating exploit results against 10 assets	Remote-asset exposure
62	26 Sep 2026 17:56 UTC	progress	status	exploit	progress (running, 70%)	n/a
63	26 Sep 2026 17:56 UTC	thinking	validation	exploit	Version check confirms the advisory match; timing and marker probes use demo markers	Vulnerability correlation
64	26 Sep 2026 17:56 UTC	progress	status	exploit	progress (running, 73%)	n/a
65	26 Sep 2026 17:56 UTC	thinking	analysis	exploit	Correlating exploit results against 10 assets	Vulnerability correlation
66	26 Sep 2026 17:56 UTC	finding	finding	infra	Outdated TLS protocol versions accepted	DNS intelligence
67	26 Sep 2026 17:56 UTC	progress	status	exploit	progress (running, 76%)	n/a

#	When	Type	Category	Phase	Summary	Capability
68	26 Sep 2026 17:56 UTC	thinking	analysis	exploit	Correlating exploit results against 10 assets	Browser attack paths
69	26 Sep 2026 17:56 UTC	progress	status	exploit	progress (running, 79%)	n/a
70	26 Sep 2026 17:56 UTC	phase	phase	exploit	Exploitability Validation complete (completed)	n/a
71	26 Sep 2026 17:56 UTC	phase	phase	review	Review and Reporting started (running)	n/a
72	26 Sep 2026 17:56 UTC	thinking	analysis	review	Correlating review results against 10 assets	n/a
73	26 Sep 2026 17:56 UTC	progress	status	review	progress (running, 82%)	n/a
74	26 Sep 2026 17:56 UTC	thinking	analysis	review	Correlating review results against 10 assets	n/a
75	26 Sep 2026 17:56 UTC	finding	finding	infra	Publicly listable cloud storage bucket	Cloud posture
76	26 Sep 2026 17:56 UTC	progress	status	review	progress (running, 85%)	n/a
77	26 Sep 2026 17:56 UTC	thinking	analysis	review	Mapping findings to ATT&CK, OWASP, NIST CSF, 800-53, 800-171 and COBIT	n/a
78	26 Sep 2026 17:56 UTC	progress	status	review	progress (running, 88%)	n/a
79	26 Sep 2026 17:56 UTC	thinking	analysis	review	Correlating review results against 10 assets	n/a
80	26 Sep 2026 17:56 UTC	progress	status	review	progress (running, 91%)	n/a
81	26 Sep 2026 17:56 UTC	thinking	analysis	review	Correlating review results against 10 assets	n/a
82	26 Sep 2026 17:56 UTC	finding	finding	recon	Dangling DNS record allows subdomain takeover	Open-source intel

#	When	Type	Category	Phase	Summary	Capability
83	26 Sep 2026 17:56 UTC	progress	status	review	progress (running, 94%)	n/a
84	26 Sep 2026 17:56 UTC	thinking	analysis	review	Scoring risk and drafting the report	n/a
85	26 Sep 2026 17:56 UTC	progress	status	review	progress (running, 97%)	n/a
86	26 Sep 2026 17:56 UTC	thinking	analysis	review	Correlating review results against 10 assets	n/a
87	26 Sep 2026 17:56 UTC	finding	finding	web	Source control metadata exposed (.git directory)	Source-code review
89	26 Sep 2026 17:56 UTC	phase	phase	review	Review and Reporting complete (completed)	n/a
90	26 Sep 2026 17:56 UTC	complete	complete	n/a	Assessment complete. Risk score 100 (completed, 100%)	n/a
105	27 Sep 2026 13:21 UTC	report	report	n/a	Report v16 ready (ready)	n/a
106	27 Sep 2026 13:22 UTC	report	report	n/a	Report v17 ready (ready)	n/a
107	27 Sep 2026 13:22 UTC	report	report	n/a	Report v18 ready (ready)	n/a
108	27 Sep 2026 13:22 UTC	report	report	n/a	Report v19 ready (ready)	n/a
109	27 Sep 2026 13:22 UTC	report	report	n/a	Report v20 ready (ready)	n/a
110	27 Sep 2026 13:22 UTC	report	report	n/a	Report v21 ready (ready)	n/a
111	27 Sep 2026 13:22 UTC	report	report	n/a	Report v22 ready (ready)	n/a
112	27 Sep 2026 13:22 UTC	report	report	n/a	Report v23 ready (ready)	n/a

#	When	Type	Category	Phase	Summary	Capability
113	27 Sep 2026 17:51 UTC	report	report	n/a	Report v24 ready (ready)	n/a
114	27 Sep 2026 17:51 UTC	report	report	n/a	Report v25 ready (ready)	n/a
115	27 Sep 2026 17:51 UTC	report	report	n/a	Report v26 ready (ready)	n/a
116	28 Sep 2026 07:31 UTC	report	report	n/a	Report v27 ready (ready)	n/a

Appendix E Report metadata and provenance

Document id	scn_cb416011e91841c3-v1
Schema version	1.0.0
Generator	aqira-gateway 0.1.0
Generated at	29 Sep 2026 09:30 UTC
Kind	professional
Template	executive-cyber
Redaction	operator identities redacted

Formats of this issue

Format	Content type	SHA-256
html	text/html; charset=utf-8	see the report library
json	application/json; charset=utf-8	see the report library
md	text/markdown; charset=utf-8	see the report library

Data sources

Source	Kind	Detail	Rows
scans	table	SCAN_SELECT WHERE s.id = \$1	1
findings	table	FINDING_SELECT via scan_findings	12
observations	table	WHERE scan_id = \$1 AND finding_id = ANY(findings)	13
finding_history	table	JOIN users for the actor; identities redacted	25
scan_findings	table	other runs of the same findings; observedAt = min(observations.observed_at)	39
assets	table	WHERE scan_id = \$1	10
asset_identities	table	span from assets.created_at per identity (critique); asset_identities.* is the fallback	10
scan_events	table	WHERE scan_id = \$1 ORDER BY seq (cap 5000)	101
reports	table	previous issues of this run	51
scans (lineage)	table	WHERE owner_id AND domain AND target_type ORDER BY created_at	4
cve_cache	table	docs of the run's CVE ids	2
cve_feed	feed	7-day window intersection	0
cve_enrichment	table	EPSS per CVE where fetched	0
compliance_controls	table	tenant-wide status, owner, note (snapshotted)	402
compliance_evidence	table	metadata only	47
scan_schedules	table	domain = scan.domain OR last_scan_id = scan.id	1
collectors	table	WHERE owner_id (no scan relation exists)	5

Source	Kind	Detail	Rows
audit_log	table	engagement actions for the run, its reports and its findings	108
portfolio	endpoint	/api/overview, /api/findings/summary, /api/scans, /api/compliance/summary, /api/cve/feed equivalents	41
attack catalogue	catalog	ATT&CK v15.1	416
owasp catalogue	catalog	OWASP Top 10 2021	10
nistcsf catalogue	catalog	NIST CSF 2.0	106
nist80053 catalogue	catalog	NIST SP 800-53 Rev 5	198
nist800171 catalogue	catalog	NIST SP 800-171 Rev 2	110
cobit catalogue	catalog	COBIT 2019	40
derivations	derived	risk, distributions, attack paths, roadmap, executive narrative (derive.js)	n/a

Catalogue versions

attack	v15.1
owasp	2021
nistcsf	2.0
nist80053	5.1.1
nist800171	r2
cobit	2019

Excluded modules

Module	Reason
cloud	Cloud posture screens are console fixtures (src/features/cloud); no gateway tables back them.
microsoft	Microsoft tenant posture and identity graph screens are console fixtures (src/features/microsoft).
code-security	SAST, secrets, dependency and SBOM screens are console fixtures (src/features/code-security).
mobile-package	APK package summary and MASVS coverage are console fixtures (src/features/mobile-apk).
threat-intel-kev	CISA KEV listings are a console fixture (src/features/threat-intel).
threat-intel-exposure	Breach and credential exposure records are a console fixture.
threat-intel-iocs	Indicators of compromise are a console fixture.
threat-intel-actors	The threat actor catalogue is a console fixture.
threat-geography	Threat map country data is a console fixture (src/features/threat-intel).
compliance-stub-frameworks	masvs, cis-aws, cis-azure, cis-gcp, cis_m365 and scuba are not correlated by the gateway.

Warnings

Code	Message	Path
epss_not_fetched	EPSS not fetched (no server-side enrichment); threat.epss is null.	/findings
kev_not_available	CISA KEV listings are not ingested by this gateway; kevListed is null.	/cves

Engagement log

When	Action	By	Target	Detail
29 Aug 2026 14:13 UTC	finding.status	operator	fnd_7c04b2955d85	to=acceptedRisk, from=open
29 Aug 2026 14:14 UTC	finding.status	operator	fnd_7f56eb6e79fe	to=acceptedRisk, from=open
29 Aug 2026 14:20 UTC	finding.status	operator	fnd_8bedb04f3623	to=acceptedRisk, from=open
29 Aug 2026 14:22 UTC	finding.status	operator	fnd_42ef2222f4ed	to=acceptedRisk, from=open
7 Sep 2026 14:18 UTC	finding.status	operator	fnd_8a62446c5a44	to=acceptedRisk, from=open
14 Sep 2026 14:13 UTC	finding.status	operator	fnd_8bedb04f3623	to=open, from=acceptedRisk
14 Sep 2026 14:14 UTC	finding.status	operator	fnd_7c04b2955d85	to=open, from=acceptedRisk
14 Sep 2026 14:15 UTC	finding.status	operator	fnd_8a62446c5a44	to=open, from=acceptedRisk
14 Sep 2026 14:16 UTC	finding.status	operator	fnd_7f56eb6e79fe	to=open, from=acceptedRisk
14 Sep 2026 14:22 UTC	finding.status	operator	fnd_42ef2222f4ed	to=open, from=acceptedRisk
21 Sep 2026 17:03 UTC	finding.status	operator	fnd_bd03fef20182	to=resolved, from=open
22 Sep 2026 17:03 UTC	finding.status	operator	fnd_62ba44d7c26e	to=falsePositive, from=open

When	Action	By	Target	Detail
23 Sep 2026 17:03 UTC	finding.status	operator	fnd_bd03fef20182	to=open, from=resolved
26 Sep 2026 23:55 UTC	report.download	operator	c2aca8b1-474e-43de-82f3-5ae56d6d7be5	format=html, version=1
27 Sep 2026 00:33 UTC	report.download	operator	c2aca8b1-474e-43de-82f3-5ae56d6d7be5	format=html, version=1
27 Sep 2026 13:06 UTC	report.forge	operator	scn_cb416011e91841c3	formats=html,pdf,json,csv, version=2, templated=executive-cyber
27 Sep 2026 13:07 UTC	report.forge	operator	scn_cb416011e91841c3	formats=html,pdf,json,csv, version=3, templated=audit-compliance
27 Sep 2026 13:07 UTC	report.forge	operator	scn_cb416011e91841c3	formats=html,pdf,json,csv, version=4, templated=boardroom-risk
27 Sep 2026 13:07 UTC	report.forge	operator	scn_cb416011e91841c3	formats=html,pdf,json,csv, version=5, templated=corporate-light
27 Sep 2026 13:07 UTC	report.forge	operator	scn_cb416011e91841c3	formats=html,pdf,json,csv, version=6, templated=cybersecurity
27 Sep 2026 13:07 UTC	report.forge	operator	scn_cb416011e91841c3	formats=html,pdf,json,csv, version=7, templated=minimal-dark
27 Sep 2026 13:07 UTC	report.forge	operator	scn_cb416011e91841c3	formats=html,pdf,json,csv, version=8, templated=minimal-formal
27 Sep 2026 13:07 UTC	report.forge	operator	scn_cb416011e91841c3	formats=html,pdf,json,csv, version=9, templated=technical-deep-dive
27 Sep 2026 13:15 UTC	report.forge	operator	scn_cb416011e91841c3	formats=html,pdf,json,csv, version=10, templated=executive-cyber
27 Sep 2026 13:15 UTC	report.forge	operator	scn_cb416011e91841c3	formats=html,pdf,json,csv, version=11, templated=boardroom-risk
27 Sep 2026 13:15 UTC	report.forge	operator	scn_cb416011e91841c3	formats=html,pdf,json,csv, version=12, templated=audit-compliance
27 Sep 2026 13:19 UTC	report.forge	operator	scn_cb416011e91841c3	formats=html,pdf,json,csv, version=13, templated=audit-compliance

When	Action	By	Target	Detail
27 Sep 2026 13:19 UTC	report.forge	operator	scn_cb416011e91841c3	formats=html,pdf,json,csv, version=14, templated=executive-cyber
27 Sep 2026 13:19 UTC	report.forge	operator	scn_cb416011e91841c3	formats=html,pdf,json,csv, version=15, templated=cybersecurity
27 Sep 2026 13:21 UTC	report.forge	operator	scn_cb416011e91841c3	formats=html,pdf,json,csv, version=16, templated=audit-compliance
27 Sep 2026 13:21 UTC	report.download	operator	83ed8f40-417e-455b-82d0- 50337e073120	format=csv, version=16
27 Sep 2026 13:21 UTC	report.preview	operator	83ed8f40-417e-455b-82d0- 50337e073120	format=csv, version=16
27 Sep 2026 13:21 UTC	report.download	operator	1f89e32e-257f-4b67-ac03- 8a04a14ac82c	format=html, version=16
27 Sep 2026 13:21 UTC	report.download	operator	de6b3dae-868e-43f9-9995- 6d13dc7447dd	format=json, version=16
27 Sep 2026 13:21 UTC	report.download	operator	18fcbad2-3c40-47e3-ad99- 8d7bd35d941b	format=pdf, version=16
27 Sep 2026 13:21 UTC	report.forge	operator	scn_cb416011e91841c3	formats=html,pdf,json,csv, version=17, templated=boardroom-risk
27 Sep 2026 13:22 UTC	report.download	operator	e8b32db7-2dbe-468f-999b- 33ed0aa972e1	format=csv, version=17
27 Sep 2026 13:22 UTC	report.preview	operator	e8b32db7-2dbe-468f-999b- 33ed0aa972e1	format=csv, version=17
27 Sep 2026 13:22 UTC	report.download	operator	7ba7ae1d-1fac-4e84-8e4f- 5b1f8e75f48a	format=html, version=17
27 Sep 2026 13:22 UTC	report.download	operator	a3a164c1-55e2-43e3-be80- 1b6b31c02d1b	format=json, version=17
27 Sep 2026 13:22 UTC	report.download	operator	3ad10fea-1632-403d-a0a4- 42664c247ccb	format=pdf, version=17
27 Sep 2026 13:22 UTC	report.forge	operator	scn_cb416011e91841c3	formats=html,pdf,json,csv, version=18, templated=corporate-light

When	Action	By	Target	Detail
27 Sep 2026 13:22 UTC	report.download	operator	3b69242b-7c82-4604-bc54-0865ec2c4624	format=csv, version=18
27 Sep 2026 13:22 UTC	report.preview	operator	3b69242b-7c82-4604-bc54-0865ec2c4624	format=csv, version=18
27 Sep 2026 13:22 UTC	report.download	operator	00b9aeb7-ba7c-4755-b6d7-1ae18dcc2b71	format=html, version=18
27 Sep 2026 13:22 UTC	report.download	operator	71fefc36-7f54-4104-b09e-d394fa77d4eb	format=json, version=18
27 Sep 2026 13:22 UTC	report.download	operator	f3e5d9c9-34cc-4ddd-b8dc-885178bcdd69	format=pdf, version=18
27 Sep 2026 13:22 UTC	report.forge	operator	scn_cb416011e91841c3	formats=html,pdf,json,csv, version=19, templateId=cybersecurity
27 Sep 2026 13:22 UTC	report.download	operator	d5a74645-91b1-4aa8-9b5e-de56d5e69d3c	format=csv, version=19
27 Sep 2026 13:22 UTC	report.preview	operator	d5a74645-91b1-4aa8-9b5e-de56d5e69d3c	format=csv, version=19
27 Sep 2026 13:22 UTC	report.download	operator	d8936230-f57f-4c1b-a2f5-016d2ff8c513	format=html, version=19
27 Sep 2026 13:22 UTC	report.download	operator	8f08d7dc-845f-48d2-bb2d-dfe11b567ea2	format=json, version=19
27 Sep 2026 13:22 UTC	report.download	operator	9efcb88d-0116-4d29-88d2-8fe88d4ead41	format=pdf, version=19
27 Sep 2026 13:22 UTC	report.forge	operator	scn_cb416011e91841c3	formats=html,pdf,json,csv, version=20, templateId=executive-cyber
27 Sep 2026 13:22 UTC	report.download	operator	e73dabad-d2ea-4502-a57e-3886667fe06c	format=csv, version=20
27 Sep 2026 13:22 UTC	report.preview	operator	e73dabad-d2ea-4502-a57e-3886667fe06c	format=csv, version=20
27 Sep 2026 13:22 UTC	report.download	operator	7cd7dc85-6cb6-4b61-92e7-67f13e43881e	format=html, version=20

When	Action	By	Target	Detail
27 Sep 2026 13:22 UTC	report.download	operator	cb331c18-924b-4288-9498-fa2fd45a4388	format=json, version=20
27 Sep 2026 13:22 UTC	report.download	operator	efc1626d-cbe5-461b-abd2-16df30091d0b	format=pdf, version=20
27 Sep 2026 13:22 UTC	report.forge	operator	scn_cb416011e91841c3	formats=html, pdf, json, csv, version=21, templated=minimal-dark
27 Sep 2026 13:22 UTC	report.download	operator	88f1deb2-a139-4c22-bdc7-bb8a9e723be5	format=csv, version=21
27 Sep 2026 13:22 UTC	report.preview	operator	88f1deb2-a139-4c22-bdc7-bb8a9e723be5	format=csv, version=21
27 Sep 2026 13:22 UTC	report.download	operator	3975819d-95f5-42a8-9102-b72b7ce8eb0d	format=html, version=21
27 Sep 2026 13:22 UTC	report.download	operator	65036ae6-0640-4802-b316-72280cab5d1c	format=json, version=21
27 Sep 2026 13:22 UTC	report.download	operator	06fe18ac-866f-468c-9a52-dc57370aefd4	format=pdf, version=21
27 Sep 2026 13:22 UTC	report.forge	operator	scn_cb416011e91841c3	formats=html, pdf, json, csv, version=22, templated=minimal-formal
27 Sep 2026 13:22 UTC	report.download	operator	4bb5cacb-4a8f-4370-a52f-656de1488916	format=csv, version=22
27 Sep 2026 13:22 UTC	report.preview	operator	4bb5cacb-4a8f-4370-a52f-656de1488916	format=csv, version=22
27 Sep 2026 13:22 UTC	report.download	operator	12ef5cea-e7c3-494d-a8a2-4ae9fa6d8574	format=html, version=22
27 Sep 2026 13:22 UTC	report.download	operator	31a769ae-df49-4d76-a150-fce587a8bec7	format=json, version=22
27 Sep 2026 13:22 UTC	report.download	operator	483020b5-8149-4732-8443-a067e1ac5fc1	format=pdf, version=22
27 Sep 2026 13:22 UTC	report.forge	operator	scn_cb416011e91841c3	formats=html, pdf, json, csv, version=23, templated=technical-deep-dive

When	Action	By	Target	Detail
27 Sep 2026 13:22 UTC	report.download	operator	5ac33a5c-13a7-4e90-b508-aa0d3e2e9c6e	format=csv, version=23
27 Sep 2026 13:22 UTC	report.preview	operator	5ac33a5c-13a7-4e90-b508-aa0d3e2e9c6e	format=csv, version=23
27 Sep 2026 13:22 UTC	report.download	operator	0b8062de-7559-431b-bf65-a10e553cecc3	format=html, version=23
27 Sep 2026 13:22 UTC	report.download	operator	cafb1f86-2b95-438e-9a90-18b8f6419d9b	format=json, version=23
27 Sep 2026 13:22 UTC	report.download	operator	3e89b40d-db43-499e-87af-d871c3a262d1	format=pdf, version=23
27 Sep 2026 17:51 UTC	report.forge	operator	scn_cb416011e91841c3	formats=html,pdf,json,csv, version=24, templateId=executive-cyber
27 Sep 2026 17:51 UTC	report.download	operator	96205236-f6ec-4224-9dfe-1ebd06964f83	format=csv, version=24
27 Sep 2026 17:51 UTC	report.download	operator	ab56f772-658c-44a8-9956-bca57c5e298e	format=html, version=24
27 Sep 2026 17:51 UTC	report.download	operator	2e07736c-54ee-4b46-884d-873394d1faf8	format=json, version=24
27 Sep 2026 17:51 UTC	report.download	operator	669d1933-2b49-4b3e-a234-f5c69784c3fd	format=pdf, version=24
27 Sep 2026 17:51 UTC	report.forge	operator	scn_cb416011e91841c3	formats=html,pdf,json,csv, version=25, templateId=technical-deep-dive
27 Sep 2026 17:51 UTC	report.download	operator	91868cea-3ec6-4038-ba40-606259605d29	format=csv, version=25
27 Sep 2026 17:51 UTC	report.download	operator	08bc9779-9066-4f78-9c0e-7ec16b831758	format=html, version=25
27 Sep 2026 17:51 UTC	report.download	operator	02333153-4182-4131-8f8c-83e1c9cd21d3	format=json, version=25
27 Sep 2026 17:51 UTC	report.download	operator	cb2eda15-a674-478e-b918-2e584b1bf222	format=pdf, version=25

When	Action	By	Target	Detail
27 Sep 2026 17:51 UTC	report.forge	operator	scn_cb416011e91841c3	formats=html,pdf,json,csv, version=26, templateId=minimal-dark
27 Sep 2026 17:51 UTC	report.download	operator	bc0aad77-70f0-443c-bab2- 5a0b2cb1e16c	format=csv, version=26
27 Sep 2026 17:51 UTC	report.download	operator	6239c079-af14-4c62-9403- f6074ed99d5b	format=html, version=26
27 Sep 2026 17:51 UTC	report.download	operator	b56f0eb4-683c-4bcc-a3a2- 3bcdffceabeb	format=json, version=26
27 Sep 2026 17:51 UTC	report.download	operator	c74c4fdc-9555-4cc6-b967- 5c7b7aae850c	format=pdf, version=26
27 Sep 2026 17:56 UTC	report.download	operator	bc0aad77-70f0-443c-bab2- 5a0b2cb1e16c	format=csv, version=26
27 Sep 2026 17:56 UTC	report.preview	operator	bc0aad77-70f0-443c-bab2- 5a0b2cb1e16c	format=csv, version=26
28 Sep 2026 07:31 UTC	report.forge	operator	scn_cb416011e91841c3	formats=html,pdf,json,csv, version=27, templateId=technical-deep-dive
28 Sep 2026 07:32 UTC	report.download	operator	82d3181e-4a16-4e1c-88db- 275506c6ce46	format=html, version=27
28 Sep 2026 07:32 UTC	report.download	operator	6eadbe98-999a-4336-bc65- 1d55cbfe8e6b	format=pdf, version=27
28 Sep 2026 07:32 UTC	report.download	operator	5bd4b6f6-6d43-470c-8ea6- 6535074de63b	format=json, version=27
28 Sep 2026 07:32 UTC	report.download	operator	f0bc674d-8389-4c2e-8edc- 3306984d5f86	format=csv, version=27
28 Sep 2026 07:32 UTC	report.preview	operator	82d3181e-4a16-4e1c-88db- 275506c6ce46	format=html, version=27
28 Sep 2026 07:32 UTC	report.preview	operator	82d3181e-4a16-4e1c-88db- 275506c6ce46	format=html, version=27
28 Sep 2026 07:43 UTC	report.download	operator	f0bc674d-8389-4c2e-8edc- 3306984d5f86	format=csv, version=27

When	Action	By	Target	Detail
28 Sep 2026 07:43 UTC	report.preview	operator	f0bc674d-8389-4c2e-8edc-3306984d5f86	format=csv, version=27
28 Sep 2026 07:43 UTC	report.download	operator	f0bc674d-8389-4c2e-8edc-3306984d5f86	format=csv, version=27
28 Sep 2026 07:43 UTC	report.preview	operator	f0bc674d-8389-4c2e-8edc-3306984d5f86	format=csv, version=27
29 Sep 2026 17:05 UTC	report.preview	operator	ab56f772-658c-44a8-9956-bca57c5e298e	format=html, version=24
29 Sep 2026 17:09 UTC	report.preview	operator	ab56f772-658c-44a8-9956-bca57c5e298e	format=html, version=24
29 Sep 2026 17:11 UTC	report.preview	operator	ab56f772-658c-44a8-9956-bca57c5e298e	format=html, version=24

CSV note: cells whose value starts with =, +, -, @, tab or a line break are prefixed with a single quote so spreadsheet software never evaluates them; strip the quote when importing programmatically.