CVE-XXXX-XXXXX on acme: notified, verified, patched and proven in 2 h 00

An authorization flaw in a self-hosted open-source tool. High, CVSS 8.1. Fixed upstream in 1.7.5 and 1.8.1. Upgrading remediates. Source: the upstream maintainers' advisory, GHSA and NVD. The flaw and the fix are theirs; the verdicts, the backport, the hunt and this record are Backportal's.

3	2	0	2 h 00
instances declared	affected and patched	indicators of exploitation	time to patch

Verdict per instance

INSTANCE	VERSION	EXPOSURE CONTEXT	VERDICT	ACTION
app-eu-1	1.6.9	internet-facing, feature enabled	affected	patched at 10:40Z
app-us-1	1.6.9	internet-facing, feature enabled	affected	patched at 10:40Z
app-internal	1.7.5	internal, feature disabled	fixed	none

Timeline

TIME (UTC)	STEP	WHAT HAPPENED
2026-09-07 09:02:11Z	Notify	Advisory CVE-XXXX-XXXXX matched declared stack: example tool on 3 instances.
2026-09-07 09:05:40Z	Assess	2 instances affected (1.6.9). 1 not affected: 1.7.5 includes the fix, and the vulnerable feature is disabled there.
2026-09-07 09:11:02Z	Verify	Exploitability check confirmed the vulnerable condition reachable on app-eu-1 and app-us-1. No attack performed.
2026-09-07 10:40:27Z	Patch	Upstream fix commits backported onto fork acme/example-tool line 1.6. Build, upstream suite and CVE regression test passed. Merge request !412 merged.
2026-09-07 10:58:13Z	Hunt	Hunt queries run on 30 days of logs and application state on both affected instances. No indicators of exploitation.
2026-09-07 11:02:45Z	Prove	Record signed. OpenVEX statements published for 3 instances. Time to patch: 2 h 00 from advisory match.

Evidence

Advisory	CVE-XXXX-XXXXX · upstream advisory, GHSA and NVD records linked · published T+0 · `backportal.dev/cve/example-tool/cve-xxxx-xxxxx`
Detection check	`checks/example-tool/cve-xxxx-xxxxx/detect.sh` · sha256 `(recorded at run time)` · run on 3 instances, level one, runner v0.3.1
Exploitability check	`checks/example-tool/cve-xxxx-xxxxx/verify.sh` · confirmed reachable on app-eu-1, app-us-1 · not run on app-internal (not affected) · no attack performed
Patch	The two upstream fix commits, credited to their authors, backported onto `acme/example-tool` line 1.6 · build passed · upstream suite passed · CVE regression test passed · merge request !412
Hunt	`hunt/example-tool/cve-xxxx-xxxxx/*.sql` · 30 days of logs and application state · 0 indicators of exploitation matched
VEX	3 OpenVEX statements: app-eu-1 fixed (patched), app-us-1 fixed (patched), app-internal not affected, justification vulnerable_code_not_in_execute_path

Signature

Signed by	acme runner key `ed25519:…(sample)` and Backportal `ed25519:…(sample)`
Record digest	`sha256:(computed at signing time, sample)`
Verify	`backportal verify rec_2026-09-07_example_acme.json`

Sources

- The upstream maintainers' security advisory (the owners of the flaw and the fix)
- The GitHub Security Advisory record
- The NVD record
- Upstream release notes and tag-to-tag diffs for 1.7.5 and 1.8.1