AXIOM CYBER RESEARCH

SAMPLE ISSUE

LEFT OF EXPLOIT BRIEF

CVE-2026-76466: a public exploit for unauthenticated root on Cisco Expressway (CVSS 9.8)

A public Python exploit exists. As of 14 November, no exploitation has been reported.

CVE-2026-76466 · CVSS 9.8 · Sample issue · 14 November 2026 · compiled from public sources; full list on the last page · This week's patch call, and what would prove it wrong.

Judgment — as of 14 November 2026

Status: left of exploit (as of 14 November 2026). No public record yet confirms exploitation; the flip condition is below.

We rate this a patch-this-week exposure check, not a confirmed campaign: the flaw gives unauthenticated remote root on Cisco Expressway, a public Python exploit has existed since November 5, and EPSS sits at 0.42% today with no exploitation reported. Patch internet-facing Expressways this week; the rest on your normal cycle.

Held if a named public record confirms exploitation by 14 December 2026 — vendor PSIRT, CISA KEV, a national CERT or a named research firm; scored wrong on the public call log if none does. Every record named is public and checkable without trusting us.

Check us yourself: EPSS was 0.42% on 14 November 2026 (api.first.org) — a dated snapshot. No verified count of internet-facing Expressways exists.

Are you exposed?

POTENTIALLY AFFECTED — check now	CHECK — confirm your version	FIXED RELEASES
Cisco Expressway Series — unauthenticated remote root via the database service, per Cisco; confirm your configuration against the PSIRT advisory. An owned Expressway carries your enterprise video and voice calling	Internet-facing or DMZ systems come first. No public count of exposed systems has been verified	Cisco advisory fixed-software table: X15.5.3 and earlier → X15.5.20

Do this, in order

1. Inventory Cisco Expressway systems and confirm the running version. (Infrastructure)
2. Upgrade internet-facing systems to X15.5.20 per the Cisco advisory's fixed-software table (X15.5.3 and earlier are affected). (Collaboration/Infrastructure)
3. Apply any configuration-specific mitigation Cisco recommends. (Security)

Additional check (Security): confirm your Expressway version and configuration against Cisco PSIRT's advisory.

Written by Robert White · Axiom Cyber Research

What the flaw is

The database service of Cisco Expressway accepts connections that rely on persistent cookies and insufficient client-certificate validation in the TLS flow; an unauthenticated remote attacker with network access to the appliance can reach a path that executes operating-system commands as root (CVSS 9.8; NVD published 2026-10-21; Cisco PSIRT advisory cisco-sa-vcs-static-cred-hr7EWZ8t).

Why it is on the radar

Date (2026)	What happened
Oct 21	NVD publishes the record; Cisco ships the fix in its October security bundle.
Nov 5	A public Python exploit with fleet-detection notes appears (dinosn/cve-2026-76466; 7 stars as of Nov 14 — early, not viral).
Nov 12	Security press picks up the PoC release (GBHackers — see sources).
Nov 14	EPSS 0.42%; not in CISA KEV; no exploitation reported. This Brief's judgment is dated today.

The shape is the reason: unauthenticated root on an edge appliance with a working public exploit. As of 14 November 2026, no incident reporting exists for this flaw. We are not saying exploitation is coming. We are saying the ingredients are public and the patch window is open.

What is not known yet

- Whether any exploitation has occurred (nothing reported as of 2026-11-14).
- How many Expressway systems are internet-facing (no verified count).
- Whether the flaw is reachable in every deployment or only specific configurations (the PSIRT advisory carries the configuration detail; we do not paraphrase it into a claim).

> **Why this Brief exists.** Each weekly Left of Exploit Brief brings affected versions, mitigations, and relevant infrastructure into one sourced assessment, with the judgment dated and checkable. This sample shows the format; regular issues are weekly.

Sources

1. NVD: CVE-2026-76466 (CVSS 9.8, description, published 2026-10-21) — nvd.nist.gov.
2. Cisco PSIRT advisory — sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vcs-static-cred-hr7EWZ8t (fetched; configuration detail lives here).
3. FIRST EPSS API: 0.00417 (0.42%), percentile 0.365, 2026-11-14.
4. CISA KEV catalog, retrieved 2026-11-14: CVE-2026-76466 NOT listed.
5. GitHub: dinosn/cve-2026-76466 (“Python exploit and fleet detection”), created 2026-11-05, 7★/0 forks as of 2026-11-14.
6. GBHackers: “PoC Exploit Released for Critical Cisco Expressway RCE Vulnerability With CVSS 9.8 Score”, 12 Nov 2026 — gbhackers.com/poc-exploit-released-for-critical-cisco-expressway-rce/ (URL verified 2026-11-17).
7. Runner-up: CVE-2026-112611 (Apple CoreGraphics PDF OOB write, PoC ≈96★) — named for transparency; auto-update blunts urgency.

Corrected 16 November 2026: the Cisco advisory identifier in two places, two wording changes, and the page footer. Corrected again 16 November 2026: the pricing line on page 2 removed; the author line and two passages on page 2 reworded. The call, its date and its test are unchanged. Corrected 17 November 2026: two unverified sources removed, one source verified, and the fixed-version line corrected to the Cisco advisory's table. Corrected 21 November 2026: the call's test sentence now matches its patch-this-week tier — wrong only if no named public record confirms exploitation by the check date. The call and its date are unchanged.