CVE-2026-76466

Cisco · Cisco Expressway first reported 12 Nov 2026 10 of 17 sources

v15 · updated 25 Nov 2026, 15:15 UTC

EXPLOITED IN THE WILD — LISTED IN CISA KEV

> *"CISA added CVE-2026-76466 to its Known Exploited Vulnerabilities (KEV) catalog on 20 November after reports emerged that the flaw was being used in active attacks."* [4]

BOTTOM LINE

A hard-coded-credentials RCE in clustered Cisco Expressway (CVE-2026-76466) allows unauthenticated root command execution; a public PoC exists and attackers have used it in the wild. Patch or migrate to fixed releases immediately or block TCP 4371–4372 until patched and hunt for Erlang log indicators. [1,2,4]

FOR THE BOARD

A critical unauthenticated vulnerability in clustered Cisco Expressway lets remote attackers gain root; prioritize patching or deny TCP 4371–4372 immediately and check logs for signs of compromise.

ARE YOU EXPOSED?

AFFECTS Cisco · Cisco Expressway — versions before the fixed releases [1,3,4]

Verify device is Expressway-C or Expressway-E, clustered, and running a release earlier than X15.5.20 or X14/earlier.

WHAT TO DO

1. **Upgrade Expressway X15.5.3 and earlier to X15.5.20, and migrate X14 or earlier to a fixed release.** [1,3]
   Cisco lists X15.5.20 as the fix for X15.5.3 and earlier and requires migration for X14 and earlier.
2. **If you cannot patch immediately, block TCP ports 4371–4372 except between trusted cluster peers.** [1,2,8]
   F6 and vendors advise restricting these ports to prevent attackers reaching the Erlang database service used in the exploit.
3. **Hunt for 'nodeup 'wombat@127.0.0.1" and Erlang system log anomalies and staged Python scripts.** [3,8]
   F6 and reporting list this log entry and script path as indicators from observed intrusions.
4. **Inventory clustered Expressway nodes, confirm cluster membership and port reachability from untrusted networks.** [1,9]
   Exposure requires clustering and network access to TCP 4371–4372; inventorying enables targeted remediation and detection.

Timeline

October 21, 2026	DISCLOSURE	disclosure [1] *“Cisco published its advisory on October 21, 2026, and the flaw carries a CVSS score of 9.8.”*
2026-11-12 PUBLISHED	DISCOVERY	PoC published [1] *“Researcher Nicolas Krassas (dinosn) posted the exploit and a fleet detector on GitHub.”*
2026-11-19 PUBLISHED	EXPLOITATION	observed exploitation (first reported case) [2] *“Hackers exploited a critical Cisco Expressway vulnerability to breach a Russian organization soon after proof-of-concept (PoC) exploit code was released publicly, according to cybersecurity firm F6.”*
2026-11-23 PUBLISHED	ADVISORY	KEV listing [4] *“CISA added CVE-2026-76466 to its Known Exploited Vulnerabilities (KEV) catalog on 20 November after reports emerged that the flaw was being used in active attacks.”*
2026-11-24 PUBLISHED	RESPONSE	Cisco advisory updated to acknowledge KEV [9] *“Cisco first disclosed the vulnerability on October 21 and updated its advisory on November 23 to acknowledge the KEV listing.”*
2026-11-25 PUBLISHED	OTHER	industry prioritization [10] *“Cisco Expressway: CVE-2026-76466, a critical vulnerability added to CISA's KEV catalog on November 20. On November 23rd, CISA flagged this flaw as actively exploited after Russian cybersecurity firm F6 spotted hackers using it to gain root privileges.”*

Affected products and versions

Expressway-C and Expressway-E clustered deployments (virtual and appliance) affected when clustered. [1]

“As Cisco Expressway Flaw Lets Attackers Execute Commands as Root reported when the advisory first appeared, both Expressway-C and Expressway-E, virtual and physical, are affected when clustered.”

Fixed in

X15.5.20 [1]

“Systems on X15.5.3 and earlier must upgrade to X15.5.20, and X14 and earlier must migrate to a fixed release.”

Exploitation

Public proof-of-concept exploit posted to GitHub by researcher Nicolas Krassas. [1]

“Researcher Nicolas Krassas (dinosn) posted the exploit and a fleet detector on GitHub.”

F6 observed exploitation against a Russian organization following PoC release; attackers breached internet-facing X15.5.3 devices. [3]

“F6 said it observed what appears to be the first case of in-the-wild exploitation of the flaw to gain remote command execution on compromised Cisco Expressway X15.5.3 devices with root privileges after a PoC exploit became publicly available.”

CISA KEV listing (added 20 November) indicating active exploitation; patch-by date for federal agencies Nov 23. [4]

“CISA added CVE-2026-76466 to its Known Exploited Vulnerabilities (KEV) catalog on 20 November after reports emerged that the flaw was being used in active attacks.”

Who is exploiting it

Unattributed attackers observed by F6; no named threat actor. [2]

“F6 did not name the victim or attribute the attack to a known threat actor.”

Reports do not attribute exploitation to a specific group; CISA flagged active exploitation. [7]

“The agency cited evidence of active exploitation for all four flaws. The CISA alert did not identify victims or link the vulnerabilities to a single campaign.”

Mitigations and detection

Block or restrict TCP ports 4371–4372 to trusted cluster peers at the firewall. [2]

“F6 recommends that organizations unable to patch immediately block connections to TCP ports 4371–4372 at the firewall, except from the IP addresses of trusted cluster nodes.”

Inventory clustered nodes, confirm software versions, isolate and investigate suspected compromised systems. [1]

“For triage, they should inventory clustered nodes, check release numbers, confirm port reachability from non-peer networks, and run the ping check on each node.”

ATT&CK techniques

T1570 **Lateral Tool Transfer** MAPPED BY NEWSROOM

from: “Following root access, the attackers are said to have undertaken efforts to move laterally across the network and use custom Python scripts to scan the network, discover accessible SMB resources, interact with SQL Server and WinRM, and access GitLab repositories in order to exfiltrate credentials and other sensitive data.” [3]

Indicators

None published in the sources.

Not known yet

- Which specific cluster nodes globally are vulnerable
- Whether all observed compromises resulted in data exfiltration

- Attribution of attackers beyond 'unattributed' F6 reports

Sources

1 **GBHackers** · 12 Nov 2026 · PoC Exploit Released for Critical Cisco Expressway RCE Vulnerability With CVSS 9.8 Score · archived copy

2 **SecurityWeek** · 19 Nov 2026 · Hackers Exploit Cisco Expressway Vulnerability Soon After PoC Release · archived copy

3 **The Hacker News** · 20 Nov 2026 · Hackers Exploit Critical Cisco Expressway Flaw, Breach Four Devices and Reach Internal Network · archived copy

4 **Infosecurity Magazine** · 23 Nov 2026 · Critical Cisco Expressway Flaw Exploited in Attacks · archived copy

5 **GBHackers** · 23 Nov 2026 · Hackers Exploit Cisco Expressway CVE-2026-76466 After Public PoC Release to Gain Root Privileges · archived copy

6 **SecurityWeek** · 23 Nov 2026 · SAP NetWeaver, Cisco Expressway Flaws Exploited in Attacks · archived copy

7 **GBHackers** · 23 Nov 2026 · CISA Warns Hackers Are Actively Exploiting Cisco, VMware, SAP, and Apache Vulnerabilities · archived copy

8 **Help Net Security** · 23 Nov 2026 · Cisco Expressway vulnerability exploited to breach internal networks (CVE-2026-76466) - Help Net Security · archived copy

9 **GBHackers** · 24 Nov 2026 · Critical Cisco Expressway RCE Vulnerability Exploited in the Wild to Execute Commands as Root · archived copy

10 **BleepingComputer (Bluesky)** · 25 Nov 2026 · InfraTrust warns of exploited supply chain flaws in network appliances · archived copy

ABOUT THIS REPORT

Compiled by Transilience Newsroom from 10 public sources. Every quotation is checked against the article it cites; 8 statements were left out because the source did not bear them out. The status is never stated more strongly than its quote shows. ATT&CK techniques marked “mapped by Newsroom” are our reading of the quoted behaviour, not the source's claim. Version 15, written 25 Nov 2026, 15:15 UTC (cve-report-2026-09-25c).