Cisco Expressway flaw CVE-2026-76466 exploited soon after public PoC



F6 reports attackers used critical Cisco Expressway flaw CVE-2026-76466 to breach an organization shortly after a public PoC appeared. Clustered Expressway Core and Edge devices are affected; Cisco has no workaround.

- CVE-2026-76466 (CVSS 9.8) allows unauthenticated remote attackers to run commands as root on Expressway Core and Edge, only when devices are clustered.
- Cisco disclosed the flaw on October 21; Expressway X15.5.20 fixes it and there are no workarounds.
- A PoC exploit was posted on GitHub, and F6 says the attack it investigated followed shortly after.
- Attackers entered through two internet-exposed X15.5.3 devices, then moved to two internal cluster nodes and used custom Python scripts for lateral movement.
- F6 suggests checking the Erlang system log and, if patching is delayed, restricting TCP ports

> 4371–4372 to trusted cluster nodes.

Cybersecurity firm F6 says attackers exploited a critical flaw in Cisco Expressway to breach an organization shortly after proof-of-concept code was published. F6 did not name the victim or link the activity to a known threat actor.

What is known

The flaw, **CVE-2026-76466** (CVSS 9.8), lets a remote attacker with network access run commands as root without authentication. It affects virtual and appliance versions of Expressway Core and Expressway Edge, but only when they are clustered. Cisco says it lies in the database service and relates to persistent cookies, which allow an attacker to issue certain RPC commands.

Cisco disclosed the issue on October 21. Its advisory has not been revised and still says Cisco is unaware of malicious use, yet a PoC has since appeared on GitHub. Cisco has not yet commented on F6's findings, according to the report.

How the attack unfolded

F6 says the attackers compromised two internet-exposed Expressway X15.5.3 devices, then pivoted to two other cluster nodes on the internal network. With root access they prepared Python scripts to scan the network, find SMB resources, interact with SQL Server and WinRM, and search GitLab repositories for credentials and sensitive data. F6 believes the scripts were edited during the attack and that the code showed signs of an AI assistant.

Fix and mitigation

Expressway X15.5.20 resolves the flaw. Cisco lists no workarounds, and customers on X14 or earlier must move to a fixed release. F6 advises organizations that cannot patch immediately to block TCP ports 4371–4372 at the firewall except from trusted cluster node addresses, and to review the Erlang system log for signs of exploitation.

What to do now

1. Identify all Expressway Core and Edge devices, confirm which are clustered, and record their versions.
2. Upgrade to X15.5.20 or later; plan migration for any X14 or earlier systems, as no workaround exists.
3. If patching must wait, block TCP ports 4371–4372 at the firewall except from trusted cluster node IPs.
4. Review the Erlang system log on Expressway devices and check for the IP addresses and file paths F6 published.
5. Hunt for lateral movement toward SMB, SQL Server, WinRM and GitLab, and rotate credentials if compromise is suspected.

6. Reduce internet exposure of Expressway devices to what collaboration access strictly requires, consistent with NCA ECC patch and vulnerability management controls.