contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

Cisco Expressway Series exploited

CVE-2026-76466 · on CISA's exploited list since 20 November 2026

Analysis Report

Anyone running Cisco Expressway-C or -E in a cluster must act — CISA's deadline of 23 November 2026 has passed. Check now whether your devices are clustered and on a vulnerable release, then upgrade …

PREPARED BY	NamiQ	DATE	25 November 2026
FACTS AS OF	25 November 2026	VERSION	1.0
SEVERITY	**Critical: CVSS 3.1 9.8**	STATUS	On CISA's exploited list; due 23 November 2026

NamiQ © 2026 NamiQ. All rights reserved. This document is the property of NamiQ. It may be shared unaltered, with attribution.
Companion article: namiq.io/insights/cisco-expressway-series-cve-2026-76466

The bottom line

> *Anyone running Cisco Expressway-C or -E in a cluster must act — CISA's deadline of 23 November 2026 has passed. Check now whether your devices are clustered and on a vulnerable release, then upgrade to X15.5.20; those on X14 and earlier must migrate to a fixed release.*

At a glance

Fact	Detail
Product	Cisco Expressway Series (CVE-2026-76466)
Severity	Critical: 9.8 (CVSS 3.1)
CISA	On its exploited list since 20 November 2026. Deadline for US federal agencies: 23 November 2026.
Chance of exploitation (EPSS)	0.01, the estimated chance in the next 30 days, as at 25 November 2026
Ransomware use	Not recorded by CISA. That is not the same as none.
Fixed in	X15.5.20 for releases X15.5.3 and earlier. X14 and earlier have no direct fix; the vendor's advisory says those customers must migrate to a fixed release.
Who looks first	Operators of Cisco Expressway-C (Core) or Expressway-E (Edge), virtual or appliance, where those devices are configured in a cluster. The record lists only clustered deployments as affected; standalone devices are not listed.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run Cisco Expressway-C or Cisco Expressway-E anywhere?	Nothing to do for this CVE.	Check whether those devices are configured in a cluster.
Are those Expressway devices configured in a cluster?	The record lists only clustered devices as affected; nothing to do.	Check the software release on each clustered device.
Is any clustered device running X15.5.3 or earlier, or X14 or earlier?	The record does not list releases above X15.5.3 as affected; nothing to do.	Upgrade to X15.5.20, or begin migration if on X14.

What it is

An unauthenticated attacker with network access who possesses the hard-coded persistent cookies can connect to the database service on a clustered Expressway device and invoke RPC commands that execute arbitrary operating system commands as root.

Why it matters

The vendor's advisory gives the CVSS score as 9.8, access vector network, no authentication required. The root cause (CWE-798) is hard-coded persistent cookies: because they are fixed, any attacker who knows the product can use them. Those cookies allow specific RPC commands on the database service, resulting in root-level command execution on the host. Our reading is that a clustered Expressway-E at the network edge gives an attacker a privileged foothold that bypasses most perimeter controls.

What the vendor's advisory says

We read one page on sec.cloudapps.cisco.com. In short:

- The vendor's advisory says there are no workarounds. It is part of an advisory group first published 21 October 2026 and refers to Cisco Expressway Series Security Hardening Release: October 2026 for other improvements and fixes in that release.
- The advisory says X14 and earlier customers must migrate; the first fixed release for X15 is X15.5.20. Advisory ID: cisco-sa-vcs-static-cred-hr7EWZ8t, first published 21 October 2026, last updated 23 November 2026.

Things people will get wrong

- If we disable clustering, the workaround is in place The vendor's advisory states explicitly that there are no workarounds. The only remediation is upgrading to X15.5.20 or migrating from X14.
- Only the internet-facing Expressway-E is at risk The record lists both Expressway-C and Expressway-E as affected when in a cluster; an attacker with internal network access could reach a clustered Expressway-C on the same estate.
- An attacker needs to steal the cookies from a session first CWE-798 means the cookies are hard-coded into the product, not generated per session or deployment. An attacker does not need to steal them from anywhere.

How we would triage it

This is our judgement.

Step 1: Find the Expressway releases you run

- Log in to each Expressway-C and Expressway-E device and find the software version on the system information page of the administration interface.
- Confirm whether each device is part of a cluster; the advisory says only clustered devices are affected.

Step 2: Identify which devices need action

- Any clustered device on X15.5.3 or earlier is in the affected range per the vendor's advisory and needs upgrading to X15.5.20.
- Any clustered device on X14 or earlier has no direct patch available; the advisory says migration to a fixed release is required.

Step 3: Upgrade or begin migration

- For X15.5.3 and earlier: upgrade to X15.5.20 following Cisco's standard upgrade procedure.
- For X14 and earlier: begin migration to a fixed release; the advisory states no patch exists for the X14 branch.

Step 4: Check for unexpected activity if the device was exposed

- Review Expressway system and service logs for root-level process executions not initiated by an administrator.
- Check for connections to the database service from IP addresses that are not known cluster peers.

To close it, read the version from the product itself, not from an old inventory, and save the output with the date. If you cannot update today, write down who owns it, the new date, and what limits exposure until then. CISA's wording adds that you should stop using the product if no mitigation is available.

Send this to your IT provider

Copy it, change the names and dates, and send it. It is a draft for you to check, not a template tested with any provider.

> *We are writing about CVE-2026-76466, a critical flaw (CVSS 9.8) in Cisco Expressway-C and Cisco Expressway-E when configured in a cluster. An unauthenticated attacker with network access and possession of hard-coded credentials can execute commands as root via the database service. The fixed release is X15.5.20 for X15.5.3 and earlier; X14 and earlier require migration. CISA required remediation by 23 November 2026. Please confirm whether we run any clustered Expressway-C or -E, which software release each is on, and whether X15.5.20 has been applied or migration is planned. We would like written confirmation of the version and fix status by [date].*

Signs it was used

An update closes the hole. It does not tell you whether someone used it first. CISA's required action points to its forensic triage requirements (BOD 26-04). Look for:

- Unexpected root-level process executions on the Expressway host that were not initiated through the administrator interface.
- Connections to the Expressway database service from IP addresses that are not known cluster peer addresses.
- Unusual RPC command invocations in Expressway service logs from unexpected source addresses.

The weakness behind it

The record classes this as CWE-798 (Use of Hard-coded Credentials).

Likely ATT&CK mapping

MITRE ATT&CK is a public catalogue of the steps attackers take, from getting in to causing damage. No source has mapped this flaw to it yet, so the steps below are our prediction from what the record says the flaw allows. They are not MITRE's, the vendor's or CISA's, and an attacker may do other things.

Steps an attacker would likely take with this flaw

The step, in plain words	Stage of an attack	Why we think so

Exploit Public-Facing Application (T1190): Breaking in through a service that faces the internet, such as a web server, VPN or login page.	Initial Access: getting in	The flaw is in the database service of Expressway-E, an edge device typically reachable over the network; exploitation over that path would likely follow this technique.
Valid Accounts (T1078): Logging in with a real account the attacker should not have, so the activity looks like normal use.	Initial Access: getting in	CWE-798 means the attacker presents hard-coded persistent cookies as authentication material; using fixed credentials embedded in the product would typically map to this technique.
Command and Scripting Interpreter (T1059): Running commands or scripts on a machine, such as a shell or PowerShell.	Execution: running the attacker's code	A successful exploit executes arbitrary OS commands as root on the underlying host, which would involve the operating system command interpreter.

How to use this: ask your IT provider which control or log would show each step, for example whether sign-in attempts from the internet are recorded. If nobody can answer, that is the gap to close first.

MITRE ATT&CK® is a registered trademark of The MITRE Corporation. Technique names are MITRE's.

The sources, in their words

CISA's catalogue entry:

> *Cisco Expressway Series contains a use of hard-coded credentials vulnerability that allows an unauthenticated, remote attacker with persistent cookies and network access to execute commands as root on a clustered device via the database service.*

The CVE record, published by Cisco on 21 October 2026:

> *A vulnerability in the database service feature of Cisco Expressway Series could allow an unauthenticated, remote attacker with network access to a Cisco Expressway device to execute arbitrary operating system commands as root. This vulnerability is due to the use of persistent cookies. Additionally, there is insufficient validation of client certificates when the TLS Verify Mode is set to Enabled for clustering, which means that client certificates are not validated. An attacker with possession of the cookies could exploit this vulnerability by connecting to the database service and invoking specific remote procedure call (RPC) commands. A successful exploit could allow the attacker ...*

The record lists 94 affected versions or ranges of Cisco TelePresence Video Communication Server (VCS) Expressway. The first 8 are below; the rest are in the CVE record, so check your version against the whole list.

- X8.11.2
- X8.6

- X8.11.3
- X8.2.2
- X8.8.3
- X8.11.0
- X12.5.2
- X8.1.1

CISA's required action:

> *Apply mitigations in accordance with vendor instructions.*

Check your own project

If you build software, you can compare what a project declares with this CVE from a terminal. The tool reads requirements files, package.json, Maven, Gradle, Cargo, CMake and Dockerfile files, runs nothing, and only the CVE id leaves your machine. Naming the CVEs needs no key.

```
lattice-scan project . --cve CVE-2026-76466
```

Each row says in-range, outside-range, undetermined or lead, with the file and line. That is evidence about what a manifest declares, not about what runs, and a person decides. The verdicts, the CSV columns and a pipeline recipe are in the guide.

Check the servers you run

The same id can be checked against a host. Run this on the machine itself, not on the laptop that deploys to it: it reads installed packages (dpkg, rpm or apk), snaps, the hardware (maker, model, firmware), the running container images with their operating system and packages, and the kernel version, compares them on the spot, and only the CVE ids leave the machine; the inventory stays on it, in ~/.lattice-scan. Naming the CVEs needs no key. Do it on each server after a deployment, and again when a new entry lands.

```
lattice-scan --cve CVE-2026-76466
```

A match is a candidate for a person to confirm, not a finding. A distribution can fix a CVE under an unchanged version number, so a match is a candidate; on Debian-family hosts the report also shows whether the package's own changelog names the CVE. By default it opens the images your containers are running and reads their operating system and package list; a deep scan (--deep, a few minutes) opens every local image and the Python, Node, Java and Ruby packages inside them; for what an image declares, use the project check on its Dockerfile.

Guide: namiq.io/lattice/guides/choose-your-channel. MCP server (io.namiq/lattice in the MCP registry): namiq.io/lattice. Package: pypi.org/project/lattice-scan, or namiq.io/apt.

What we do not know yet

- The sources do not state whether the database service port is exposed to the internet by default or is reachable only within a cluster's internal network.
- The sources do not state whether the hard-coded persistent cookies are identical across all Expressway deployments or vary between clusters.
- The sources do not confirm whether version ranges between X14 and X15.5 exist as separate branches or how they are classified in the full advisory Fixed Software table.
- We have not tested this against any environment. Versions and scores are as the sources state them and as at 25 November 2026; the vendor's advisory wins where it differs.
- The sections headed "The bottom line", "Does this apply to you?", "What it is", "Why it matters", "Exposure by situation", "Things people will get wrong", "Likely ATT&CK mapping", "How we would triage it" and "Send this to your IT provider" are our interpretation of the sources, not a statement by CISA or the vendor.

Appendix 1. Severity decoded

CVE-2026-76466: score 9.8, `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H` As the CVE record gives it. The record's own score can differ from the base score on the NVD record.

Metric	Value	What it means here
Attack vector	Network	Reachable over a network, with no need to be on the same segment.
Attack complexity	Low	No special conditions beyond the flaw itself.
Privileges required	None	No account is needed.
User interaction	None	No one has to do anything.
Scope	Unchanged	Damage stays inside the vulnerable component.
Confidentiality	High	Total loss of confidentiality.
Integrity	High	Total loss of integrity.
Availability	High	Total loss of availability.

Appendix 2. Timeline

Date	Event
21 October 2026	CVE record published by Cisco.
20 November 2026	CISA added it to its list of exploited vulnerabilities.
23 November 2026	CISA's deadline for US federal agencies.

Appendix 3. Exposure by situation

These priorities are our judgement from the attacker prerequisites in the sources. They are not vendor ratings.

Your situation	Priority	Timeframe
Clustered Expressway-E (edge) reachable from the internet on a vulnerable release	High	Immediately — CISA deadline passed 23 November 2026
Clustered Expressway-C or -E on X14 or earlier (no direct patch; migration required)	High	Immediately; migration plan needed now
Clustered Expressway on X15.5.3 or earlier (can upgrade directly to X15.5.20)	High	Immediately — CISA deadline passed 23 November 2026

Expressway-C or -E not configured in a cluster	None	None for this CVE

Appendix 4. Definition of done

- Every Cisco Expressway Series you run is listed, with its version.
- Each is outside the affected list, or the vendor's mitigation is in place.
- The version output or a screenshot is saved with the date.
- Your projects' declared dependencies were checked against this CVE, and every row has a written reason.
- Logs for the weeks before the update were searched, and anything odd was written down.
- Anything not done has an owner and a date.

Sources

- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- CVE record for CVE-2026-76466: https://www.cve.org/CVERecord?id=CVE-2026-76466
- FIRST: Exploit Prediction Scoring System: https://www.first.org/epss/
- Advisory or release notes read: sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/c: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vcs-static-cred-hr7EWZ8t