



Advisory NCSC-2026-0451

PRIORITEIT: NORMAAL

Kwetsbaarheden verholpen in Cisco Expressway Series

Publicatiedatum: 22-10-2026

Toegestane verspreiding: TLP:WHITE
(Traffic Light Protocol)

Deze publicatie bevat het label TLP:WHITE en wordt door het Nationaal Cyber Security Center (NCSC) verspreid. Het NCSC gebruikt het Traffic Light Protocol (TLP) om eenduidig te definiëren wat er met de informatie mag gebeuren. Wanneer informatie is voorzien van een TLP-aanduiding weet u met wie u deze informatie mag delen. Dit staat beschreven in de standaard First (www.first.org/tlp).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Reacties zijn welkom op info@ncsc.nl.

Feiten

Cisco heeft meerdere kwetsbaarheden verholpen in Cisco Expressway Series.

Duiding

De kwetsbaarheden betreffen onder andere onvoldoende autorisatiecontroles tijdens Mobile en Remote Access provisioning, waardoor ongeauthenticeerde externe aanvallers toegang kunnen krijgen tot gevoelige informatie. Daarnaast is er een kwetsbaarheid in de databaseservice die het mogelijk maakt voor ongeauthenticeerde aanvallers met netwerktoegang om root-commando's uit te voeren via onvoldoende validatie van clientcertificaten bij TLS Verify Mode voor clustering.

Verder zijn er diverse kwetsbaarheden geïdentificeerd door interne security reviews, waaronder problemen met improper resource control, authenticatie, input validatie, SQL-injectie, access control, pathname limitation, exception handling, out-of-bounds write, reachable assertions, null pointer dereference, uncaught exceptions, code injection, incorrect permission assignments, improper link resolutions en insecure handling of temporary files. Deze kwetsbaarheden kunnen leiden tot het omzeilen van toegangscontroles, het uitvoeren van ongeautoriseerde code, het verkrijgen van root-toegang en het blootstellen van gevoelige data. De kwetsbaarheden zijn intern ontdekt en worden aangepakt met software hardening updates.

Oplossingen

Cisco heeft software hardening updates uitgebracht om de diverse kwetsbaarheden in Cisco Expressway Series te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-access-PW9e8Jt2>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expressway-inf-disc-vvYqgSTS>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-exwy-hardening-FhcqBVcs>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-notice-QGwHnJ6k>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vcs-static-cred-hr7EWZ8t>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-voice-hardening-twgbH9e3>

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-76435	5.3 MEDIUM
CVE-2026-76466	9.8 CRITICAL
CVE-2026-76473	9.8 CRITICAL
CVE-2026-76474	9.8 CRITICAL
CVE-2026-76475	9.3 CRITICAL
CVE-2026-76476	8.8 HIGH
CVE-2026-76477	8.8 HIGH
CVE-2026-76478	8.8 HIGH
CVE-2026-76479	7.8 HIGH
CVE-2026-76481	7.5 HIGH
CVE-2026-76487	5.3 MEDIUM
CVE-2026-76490	8.6 HIGH
CVE-2026-76491	7.5 HIGH
CVE-2026-76492	7.5 HIGH
CVE-2026-76493	7.5 HIGH
CVE-2026-76494	7.8 HIGH
CVE-2026-76495	7.8 HIGH
CVE-2026-76496	7.0 HIGH
CVE-2026-76497	6.6 MEDIUM

CWE's

CWE	Beschrijving
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
CWE-59	Improper Link Resolution Before File Access ('Link Following')
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
CWE-94	Improper Control of Generation of Code ('Code Injection')
CWE-248	Uncaught Exception
CWE-377	Insecure Temporary File
CWE-476	NULL Pointer Dereference
CWE-497	Exposure of Sensitive System Information to an Unauthorized Control Sphere
CWE-617	Reachable Assertion
CWE-732	Incorrect Permission Assignment for Critical Resource
CWE-749	Exposed Dangerous Method or Function
CWE-787	Out-of-bounds Write
CWE-798	Use of Hard-coded Credentials

Getroffen producten

Cisco
Cisco Unified Communications Manager
Expressway
Expressway Series

Disclaimer

The Netherlands Cyber Security Center (henceforth: NCSC-NL) maintains this page to enhance access to its information and security advisories. The use of this security advisory is subject to the following terms and conditions:

NCSC-NL makes every reasonable effort to ensure that the content of this page is kept up to date, and that it is accurate and complete. Nevertheless, NCSC-NL cannot entirely rule out the possibility of errors, and therefore cannot give any warranty in respect of its completeness, accuracy or continuous keeping up-to-date. The information contained in this security advisory is intended solely for the purpose of providing general information to professional users. No rights can be derived from the information provided therein. NCSC-NL and the Kingdom of the Netherlands assume no legal liability or responsibility for any damage resulting from either the use or inability of use of this security advisory. This includes damage resulting from the inaccuracy or incompleteness of the information contained in the advisory. This security advisory is subject to Dutch law. All disputes related to or arising from the use of this advisory will be submitted to the competent court in The Hague. This choice of means also applies to the court in summary proceedings.