



Advisory NCSC-2026-0409

PRIORITEIT: NORMAAL

Kwetsbaarheden verholpen in Cisco APIC

Publicatiedatum: 09-10-2026

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 Application Policy Infrastructure Controller (APIC).

Duiding

De kwetsbaarheden betreffen onder andere onvoldoende inputvalidatie in de webgebaseerde management API, waardoor een geauthenticeerde aanvaller met geldige administratieve rechten willekeurige commando's met rootprivileges kan uitvoeren. Daarnaast is er een probleem in de export policies functionaliteit die onvoldoende toegangsbescherming biedt, wat kan leiden tot ongeautoriseerde toegang tot gevoelige bestanden en privilege-escalatie naar rootniveau. Verder zijn er kwetsbaarheden geïdentificeerd die verband houden met onjuiste toegangcontrole, onjuiste neutralisatie van invoer en onjuiste resourcecontrole. Deze kunnen door een aanvaller worden misbruikt om de beveiliging van het systeem te omzeilen of systeembronnen onjuist te beheren.

Oplossingen

Cisco heeft updates uitgebracht om de kwetsbaarheden te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-apic-cmdinj-L6VR4E7>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-apic-info-priv-enAdB5vD>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-apic-UOXWtfh>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-notice-fBn58ELx>

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-20321	6.5 MEDIUM
CVE-2026-76488	6.5 MEDIUM
CVE-2026-76498	9.8 CRITICAL
CVE-2026-76499	9.8 CRITICAL
CVE-2026-76500	9.8 CRITICAL

CWE's

CWE	Beschrijving
CWE-544	Missing Standardized Error Handling Mechanism

Getroffen producten

Cisco
Cisco Application Policy Infrastructure Controller (APIC)

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.