Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0297

Kwetsbaarheden verholpen in Cisco IOS en Cisco IOS XE Software

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 25-09-2025
Revisie: 1.0.1

TLP:WHITE

Toegestane verspreiding van TLP:WHITE
(Traffic Light Protocol)

Deze handreiking bevat het label TLP:WHITE en wordt door het 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.

Uw reacties zijn welkom op info@ncsc.nl

Update Revisie 1

CVE-2025-20352 blijkt actief te zijn misbruikt. Deze informatie toegevoegd.

Feiten

Cisco heeft kwetsbaarheden verholpen in Cisco IOS en Cisco IOS XE Software.

Duiding

De kwetsbaarheden omvatten verschillende problemen, waaronder een buffer overflow in de command-line interface (CLI) die kan leiden tot onverwachte herstarts van apparaten en een kwetsbaarheid in de TACACS+ protocolimplementatie die ongeauthenticeerde aanvallers in staat stelt om gevoelige gegevens te benaderen. Daarnaast zijn er kwetsbaarheden in de web UI die kunnen leiden tot cross-site scripting (XSS) aanvallen en een probleem in de NBAR-functie dat kan resulteren in een denial of service (DoS) door het versturen van gemanipuleerde CAPWAP-pakketten. Ook zijn er kwetsbaarheden in de SNMP-subsystemen die kunnen leiden tot ongeautoriseerde toegang en systeemdisruptie.

Cisco vermeldt dat de kwetsbaarheid met kenmerk CVE-2025-20352 actief is misbruikt. Deze kwetsbaarheid stelt een kwaadwillende die in het bezit is van een read-only community string (SNMPv1/2) of geldige authenticatie (SNMPv3) een Denial-of-Service kan veroorzaken, of mogelijk willekeurige commando's kan uitvoeren met root-rechten. Voor dat laatste dient de kwaadwillende wel over administrator-rechten te beschikken.

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-9800cl-openscep-SB4xtxzP
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cat9k-PtmD7bgy
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cat9k-acl-L4K7VXgD
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-cli-EB7cZ6yO
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-invalid-url-dos-Nvxszf6u
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-tacacs-hdB7thJw

› https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xe-cmd-inject-rPJM8BGL
› https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-arg-inject-EyDDbh4e
› https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nbar-dos-LAvwTmeT
› https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-secboot-UqFD8AvC
› https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snmp-x4LPhte
› https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snmpwred-x3MJyf5M
› https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-xss-VWyDgjOU

Kwetsbaarheden

CVE	CVSS Score
› CVE-2025-20149	6.5 MEDIUM
› CVE-2025-20160	8.1 HIGH
› CVE-2025-20240	6.1 MEDIUM
› CVE-2025-20293	5.3 MEDIUM
› CVE-2025-20311	7.4 HIGH
› CVE-2025-20312	7.7 HIGH
› CVE-2025-20313	6.7 MEDIUM
› CVE-2025-20314	6.7 MEDIUM
› CVE-2025-20315	8.6 HIGH
› CVE-2025-20316	5.3 MEDIUM
› CVE-2025-20327	7.7 HIGH
› CVE-2025-20334	8.8 HIGH
› CVE-2025-20338	6.0 MEDIUM
› CVE-2025-20352	7.7 HIGH

CWE's

CWE	Beschrijving
CWE-19	CWE-19
CWE-35	Path Traversal: '.../...//'
CWE-77	Improper Neutralization of Special Elements used in a Command ('Command Injection')
CWE-120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')
CWE-121	Stack-based Buffer Overflow
CWE-141	Improper Neutralization of Parameter/Argument Delimiters
CWE-232	Improper Handling of Undefined Values
CWE-284	Improper Access Control
CWE-287	Improper Authentication
CWE-459	Incomplete Cleanup
CWE-692	Incomplete Denylist to Cross-Site Scripting
CWE-805	Buffer Access with Incorrect Length Value
CWE-835	Loop with Unreachable Exit Condition ('Infinite Loop')
CWE-1287	Improper Validation of Specified Type of Input

Getroffen producten

Cisco
Cisco 1000 Series Integrated Services Routers
Cisco 1100 Series Industrial Integrated Services Routers
Cisco 4000 Series Integrated Services Routers
Cisco Cloud Services Router 1000V Series
Cisco IOS XE Catalyst SD-WAN

IOS
iOS XE

Disclaimer