Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0210

Kwetsbaarheid verholpen in Cisco Unified Communications Manager

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 03-07-2025

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

Feiten

Cisco heeft een kwetsbaarheid verholpen in Cisco Unified Communications Manager (en Cisco Unified Communications Manager Session Management Edition).

Duiding

De kwetsbaarheid bevindt zich in de hardcoded root SSH-credentials die niet kunnen worden gewijzigd of verwijderd. Dit stelt ongeauthenticeerde externe aanvallers in staat om in te loggen en willekeurige commando's uit te voeren op de getroffen systemen. Dit vormt een ernstig beveiligingsrisico voor organisaties die deze producten gebruiken.

SSH toegang is onder normale omstandigheden beperkt tot de interne infrastructuur. Het is goed gebruik een dergelijke toegang te beperken en niet publiek toegankelijk te hebben, maar af te steunen in een separate beheer-omgeving.

Potentieel misbruik kan worden gedetecteerd door middel van de onderstaande Indicators of Compromise:

Succesvol misbruik resulteert in een log entry in `/var/log/active/syslog/secure` voor de `root` gebruiker met `root permissions`. Het loggen van dit event is standaard ingeschakeld.

De logs kunnen worden verkregen door de volgende commando's uit te voeren op de command line:

```
cucm1# file get activelog syslog/secure
```

Wanneer een log entry zowel een sshd vermelding als een succesvolle SSH login vertoont kan dit duiden op mogelijke compromittatie. Zie voorbeeld:

```
Apr 6 10:38:43 cucm1 authpriv 6 systemd: pam_unix(systemd-user:session): session opened for user root by (uid
Apr 6 10:38:43 cucm1 authpriv 6 sshd: pam_unix(sshd:session): session opened for user root by (uid=0)
```

Oplossingen

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

Referenties

› https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-ssh-m4UBdpE7

Kwetsbaarheden

CVE	CVSS Score
CVE-2025-20309	9.3 CRITICAL

CWE's

CWE	Beschrijving
CWE-798	Use of Hard-coded Credentials

Getroffen producten

Cisco
Cisco Unified Communications Manager

Disclaimer