TLP:CLEAR
Szabadon terjeszthető!

Riasztás
Cisco Catalyst SD-WAN rendszereket érintő kritikus sérülékenységről

Tisztelt Ügyfelünk!

A Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézet (NBSZ NKI) riasztást ad ki a **Cisco Catalyst SD-WAN Controller** (korábban vSmart) és **a Cisco Catalyst SD-WAN Manager** (korábban vManage) rendszereket érintő, **CVE-2026-20127** azonosítón nyomon követett, **kritikus súlyosságú** (CVSS 10.0) sérülékenység kapcsán.

Sikeres kihasználás esetén egy nem hitelesítetti támadó megkerülheti a peering-alapú hitelesítési mechanizmust, és adminisztrátori jogosultságot szerezhet egy magas jogosultsági szinttel rendelkező, de nem root, felhasználói fiókon keresztül.

A probléma a peering hitelesítési mechanizmus hibás működéséből ered, amely lehetővé teszi egy hamis peer létrehozását a menedzsment- vagy vezérlősíkon. Ennek eredményeként a támadók legitim SD-WAN komponensként jelenhetnek meg, és megbízható műveleteket hajthatnak végre a hálózaton. Ez különösen nagy kockázatot jelent a kritikus infrastruktúrát üzemeltető szervezetek számára.

A sérülékenység az **alábbi üzemeltetési modelleket** érinti:

- On-Prem alkalmazás
- Cisco hosztolt SD-WAN Cloud
- Cisco hosztolt SD-WAN Cloud – Cisco Managed
- Cisco hosztolt SD-WAN Cloud – FedRAMP Environment

Javítások és érintett verziók:

A sérülékenységet a gyártó tájékoztatása szerint az **alábbi Cisco Catalyst SD-WAN szoftververziókban javították**:

- 9.1 előtti verziók (frissítés szükséges javított kiadásra)
- 9 – 20.9.8.2 (várható kiadás: 2026. február 27.)
- 11.1 – 20.12.6.1
- 12.5 – 20.12.5.3
- 12.6 – 20.12.6.1
- 13.1 – 20.15.4.2
- 14.1 – 20.15.4.2

- 15 – 20.15.4.2
- 16.1 – 20.18.2.1
- 18 – 20.18.2.1

Javasolt intézkedések

- A sérülékenység jellege miatt javasolt **az érintett rendszerek haladéktalan frissítése** a gyártó által közzétett javított kiadásokra, különösen azon telepítések esetében, ahol a menedzsment- vagy vezérlősík szolgáltatásai közvetlenül elérhetők az internet felől.
- Ezzel párhuzamosan szükséges **a jogosulatlan felhasználói fiókok és ismeretlen SSH kulcsok felkutatása és eltávolítása**, a tartósságot szolgáló módosítások (például indítási szkriptek) ellenőrzése, valamint az adminisztratív hozzáférések és a menedzsment interfészek elérésének felülvizsgálata,
- **Célzott napló- és konfiguráció-ellenőrzést végezni**, valamint a kitettséget haladéktalanul csökkenteni.
- A /var/log/auth.log **hitelesítési naplók áttekintése**, különös tekintettel az „Accepted publickey for vmanage-admin” jellegű bejegyzésekre.
- A **naplókban szereplő forrás IP-címek összevetése** a Cisco Catalyst SD-WAN Manager felületén elérhető System IP konfigurációval (WebUI > Devices > System IP) a váratlan, nem ismert rendszerelemek azonosítása érdekében.
- Javasolt az **észlelés erősítése** (naplóvédelem, központosított naplógyűjtés), a kompromittálódás gyanúja esetén pedig incidenskezelési eljárásrend szerinti izolálás és forenzikus mentés végrehajtása.

Nemzetbiztonsági Szakszolgálat
Nemzeti Kiberbiztonsági Intézet
Telefon: +36-1-336-4833