



Riasztás a Cisco Catalyst SD-WAN Manager rendszert érintő sérülékenységről

Tisztelt Ügyfelünk!

A Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézete riasztást ad ki a Cisco Catalyst SD-WAN Manager API-jának hitelesítését érintő, aktívan kihasznált kritikus sérülékenység miatt. A hibát a Cisco közlése szerint 2026 szeptemberében már aktívan kihasználták.

A [CVE-2026-76504](#) azonosítón nyomon követett, kritikus hiba az API munkamenet-alapú hitelesítéskezelésében van. A szoftver nem megfelelően kezeli az URI-kódolást a HTTP-kérésekben, ezért a kérés megkerülhet egy, az adott API-végpontot védeni hivatott hitelesítési szabályt. Hitelesítés nélküli, távoli támadó egyetlen speciálisan összeállított HTTP-kéréssel rendszergazdai jogosultságot szerezhet. Ehhez csak hálózati elérés kell a Manager API-jához. A Manager az egész SD-WAN-hálózatot vezérli, ezért a sikeres támadás a teljes hálózat integritását és bizalmasságát veszélyezteti.

Érintett rendszerek

A sérülékenység a Cisco Catalyst SD-WAN Manager terméket érinti, a rendszerkonfigurációtól függetlenül. Sérülékenyek a következő kiadási ágak azon verziói, amelyek a javított kiadás előttiek:

Kiadási ág	Első javított kiadás
20.9 előtti kiadások	Áttérés javított kiadásra szükséges
20.9	20.9.10.1
20.12	20.12.8.2
20.15	20.15.6.1
20.18	20.18.4.1
26.1	26.1.2.1
26.2	26.2.1

A Cisco által üzemeltetett felhős példányoknál (Cloud Hosted, Cisco Managed) a javítás már megtörtént, felhasználói teendő nincs.





Javítás és kockázatcsökkentés

Szükséges a frissítés a vonalnak megfelelő javított kiadásra. Régebbi verziókról át kell térni egy javított ágra.

Ha a frissítés azonnal nem lehetséges, korlátozni kell a hozzáférést megbízható gazdagépekre, és szűrőeszköz mögé kell tenni a vezérlő komponenseket. A sérülékenységre nincs végleges megoldást jelentő workaround. Az on-prem (saját üzemeltetésű) környezetekben azonban az alábbi kockázatcsökkentő intézkedések alkalmazhatók:

- Korlátozni kell a rendszer elérését a nem megbízható hálózatokról, például az internetről.
- Ha az internetről is szükséges az elérés, azt csak ismert, megbízható gazdagépekre szabad korlátozni. Ezek a felhasználói útmutatókban szereplő portokra és protokollokra vonatkozhatnak.
- A Catalyst SD-WAN vezérlő komponenseket tűzfal (szűrőeszköz) mögé kell helyezni. A rendszerhez és a rendszertől irányuló forgalmat szűrni kell, és csak ismert, megbízható gazdagépek forgalmát szabad engedélyezni.

Kompromittálódás ellenőrzése

A Cisco két naplófájlban a j_security_check útvonalra irányuló, ismeretlen vagy jogosulatlan IP-címről érkező bejegyzéseket vizsgálatát javasolja:

- serviceproxy-access.log (/var/log/nms/containers/service-proxy/serviceproxy-access.log).
- vmanage-server.log (/var/log/nms/vmanage-server.log).

A legfrissebb információkért kérjük ügyfeleinket, hogy folyamatosan kövessék a Nemzeti Kiberbiztonsági Intézet weboldalát.

