



Riasztás

Cisco szoftvereket érintő sérülékenységekről

Tisztelt Ügyfelünk!

A Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézet riasztást ad ki a Cisco Identity Services Engine (ISE) és az ISE Passive Identity Connector (ISE-PIC) termékeket érintő, [CVE-2026-76460](#) azonosítón nyomon követett kritikus sérülékenység kapcsán. A sebezhetőség kihasználásával a támadók hitelesítés nélkül jogosulatlan hozzáférést szerezhetnek az érintett rendszerhez.

A Cisco tájékoztatása szerint a sérülékenység oka, hogy az egyik API-végpont nem megfelelően ellenőrzi a hitelesítést. A támadó egy speciálisan kialakított HTTP-kéréssel megkerülheti a webes kezelőfelület hitelesítési mechanizmusát. Sikeres kihasználás esetén a támadók root jogosultságú parancsokat is végrehajthatnak, így akár a kompromittálódás nyomait és az arra utaló jeleket is eltávolíthatják vagy elrejtik.

A sérülékenység a Cisco Identity Services Engine (ISE) és a Cisco ISE Passive Identity Connector (ISE-PIC) rendszereket egyaránt érinti, a konfigurációtól függetlenül. A hibát az alábbi verziókban javították:

- 3.1 - 3.1 Patch 12
- 3.2 - 3.2 Patch 11
- 3.3 - 3.3 Patch 12
- 3.4 - 3.4 Patch 7
- 3.5 - 3.5 Patch 4

Javasolt intézkedések:

- az érintett rendszerek frissítése,
- az access.log naplók ellenőrzése gyanús felhasználónevek keresésére,
- elosztott telepítés esetén minden csomópont naplójának vizsgálata.





TLP: CLEAR

Szabadon terjeszthető!

Amennyiben kompromittálódásra utaló jelek találhatók, a Cisco az érintett csomópontok tiszta állapotból történő újratelepítését, majd szükség esetén konfigurációs mentésből történő helyreállítását javasolja.

A CISA 2026. szeptember 16-án a CVE-2026-76460 azonosítójú sérülékenységet felvette az ismerten kihasznált sérülékenységek (Known Exploited Vulnerabilities, KEV) katalógusába.

A CVE-2026-76460 mellett a Cisco több, termékportfólióját érintő sérülékenységhoz is kiadta a szükséges javításokat, köztük a [CVE-2026-20333](#), [CVE-2026-20334](#), [CVE-2026-20332](#), [CVE-2026-20335](#), [CVE-2026-20330](#) valamint a [CVE-2026-20329](#) azonosítón nyomon követett sérülékenységekhez is.

Hivatkozások:

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-ABP-VNSW7Tn5>

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-asafdfmc-uvpPROhN>

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

Nemzetbiztonsági Szakszolgálat

Nemzeti Kiberbiztonsági Intézet

Telefon: +36-1-336-4833

Incidensbejelentés: csirt@nki.gov.hu

TLP: CLEAR

Szabadon terjeszthető!

