NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

SECURITY BULLETIN

Týždeň 02. 08. 2017 – 08. 08. 2017

No: B20170808-01V

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**
Klasifikácia	☒ **TLP (WHITE)**	☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)				

Identifikátor

Cisco Videoscape Distribution Suite Cache Server Denial of Service Vulnerability

Popis

Zraniteľnosť v cache serveri v systéme Cisco Video Distribution Suite (VDS) for Television by mohla umožniť neoverenému vzdialenému útočníkovi, aby spôsobil neprístupnosť služby (DoS) na cielenom zariadení.

Zraniteľnosť je spôsobená nadmernými mapovanými pripojeniami, ktoré zaťažujú prostriedky v systéme. Útočník by túto chybu zabezpečenia mohol zneužiť odoslaním veľkého množstva požiadaviek do zariadenia s úmyslom preťaženia určitých zdrojov. Úspešné zneužitie môže spôsobiť opätovné načítanie zariadenia, čo má za následok stav DoS.

Spoločnosť Cisco vydala aktualizácie softvéru, ktoré riešia túto zraniteľnosť. Neexistujú žiadne zástupné riešenia, ktoré by riešili túto zraniteľnosť.

CVE

CVE-2017-6745

Cisco bug ID

CSCvc39260

Zasiahnuté systémy

Cisco Videoscape Distribution Suite (VDS) for Television

Následky

Neprístupnosť služby (DoS)

Odporúčania

Spoločnosť Cisco vydala bezplatné aktualizácie softvéru, ktoré riešia predmetnú zraniteľnosť. Ak využívate tento produkt, bezodkladne aktualizujte svoje zariadenie.

Zdroje

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170802-vds

NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

SECURITY BULLETIN

Týždeň 02. 08. 2017 – 08. 08. 2017

No: B20170808-02V

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**
Klasifikácia	☒ **TLP (WHITE)**	☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)				

Identifikátor

Cisco Identity Services Engine Authentication Bypass Vulnerability

Popis

Zraniteľnosť v autentifikačnom module služby Cisco Identity Services Engine (ISE) by mohla umožniť neoverenému vzdialenému útočníkovi obísť lokálnu autentifikáciu.
Zraniteľnosť je spôsobená nesprávnym spracovaním žiadostí o overenie a priradením pravidiel pre externe overených používateľov. Útočník by túto chybu zabezpečenia mohol zneužiť autentifikáciou pomocou platného externého používateľského konta, ktorý zodpovedá internému používateľskému menu a nesprávne prijíma autorizačné pravidlá interného účtu. Expolit by mohol dovoliť útočníkovi mať orpávnenia Super Admin pre portál ISE Admin.
Táto chyba zabezpečenia neovplyvňuje koncové body autentifikácie ISE.
Spoločnosť Cisco vydala aktualizácie softvéru, ktoré riešia túto zraniteľnosť. Neexistujú žiadne zástupné riešenia, ktoré by riešili túto zraniteľnosť.

CVE

CVE-2017-6747

Cisco bug ID

CSCvb10995

Zasiahnuté systémy

Ovplyvnené sú produkty Cisco Identity Services Engine (ISE) vo verziách 1.3, 1.4, 2.0.0, 2.0.1 alebo 2.1.0. Verzie 2.2.x nie sú ovplyvnené.

Následky

Neoprávnený prístup do systému

Odporúčania

Spoločnosť Cisco vydala bezplatné aktualizácie softvéru, ktoré riešia predmetnú zraniteľnosť. Ak využívate tento produkt, bezodkladne aktualizujte svoje zariadenie.

Zdroje

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170802-ise