NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

SECURITY BULLETIN

Týždeň 26. 07. 2017 – 01. 08. 2017

No: B20170801-01V

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

Identifikátor

Cisco IOS and IOS XE Software Autonomic Networking Infrastructure Denial of Service Vulnerability

Popis

Zraniteľnosť vo funkcii Autonomic Networking softvéru Cisco IOS a softvéru Cisco IOS XE by mohla umožniť neoverenému útočníkovi spôsobiť opätovné načítanie autonómnych uzlov napadnutého systému, čo by viedlo k neprístupnosti služieb (DoS).
Zraniteľnosť je spôsobená neznámou chybou v kóde Autonomic Networking príslušného softvéru. Útočník by túto chybu zabezpečenia mohol využiť tým, že prehrá zachytené pakety na obnovenie kanálu Autonomic Control Plane (ACP) postihnutého systému. Úspešný exploit by mohol dovoliť útočníkovi, aby resetoval kanál ACP dotknutého systému a následne spôsobil opätovné načítanie dotknutého zariadenia, čo by malo za následok stav DoS.
Spoločnosť Cisco neuvoľnila aktualizácie softvéru, ktoré riešia túto zraniteľnosť. Neexistujú žiadne alternatívne riešenia, ktoré by riešili túto zraniteľnosť.

CVE

CVE-2017-6663

Cisco bug ID

CSCvd88936

Zasiahnuté systémy

Táto zraniteľnosť sa týka zariadení, ktoré používajú akékoľvek vydanie softvéru Cisco IOS alebo Cisco IOS XE, ktoré podporujú Autonomic Networking a sú nakonfigurované na používanie Autonomic Networking.

Následky

Neprístupnosť služby (DoS)

Odporúčania

Nakoľko spoločnosť CISCO doposiaľ nevydala aktualizáciu, ktorý by zahŕňal opravu tejto zraniteľnosti, odporúčame sledovať jednotlivé update zasiahnutého softvéru a po vydaní príslušnej aktualizácie ihneď túto na zasiahnuté zariadenia nainštalovať.

Zdroje

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170726-anidos

NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

SECURITY BULLETIN

Týždeň 26. 07. 2017 – 01. 08. 2017

No: B20170801-02V

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

Identifikátor

Cisco IOS and IOS XE Software Autonomic Control Plane Channel Information Disclosure Vulnerability

Popis

Zraniteľnosť vo funkcii Autonomic Networking softvéru Cisco IOS a softvéru Cisco IOS XE môže umožniť neoverenému útočníkovi obnoviť Autonomic Control Plane (ACP) postihnutého systému a prezrieť pakety ACP, ktoré sa prenášajú v čistom texte v postihnutom systéme.
Zraniteľnosť je spôsobená neznámymi dôvodmi. Útočník by mohol zneužiť túto chybu zachytávaním a prehrávaním paketov ACP, ktoré sa prenášajú v postihnutom systéme. Úspešné zneužitie by mohlo dovoliť útočníkovi, aby vynuloval ACP postihnutého systému, čoho dôsledkom je stav zamietnutia služby (DoS). Úspešné zneužitie by tiež umožnilo útočníkovi zachytiť a zobraziť pakety ACP, ktoré by mali byť zašifrované cez ACP, v jasnom texte.

CVE

CVE-2017-6665

Cisco bug ID

CSCvd51214

Zasiahnuté systémy

Táto zraniteľnosť sa týka zariadení, ktoré používajú akékoľvek vydanie softvéru Cisco IOS alebo Cisco IOS XE, ktoré podporujú Autonomic Networking a sú nakonfigurované na používanie Autonomic Networking.

Následky

Neprístupnosť služby (DoS), únik dát

Odporúčania

Nakoľko spoločnosť CISCO doposiaľ nevydala aktualizáciu, ktorý by zahŕňal opravu tejto zraniteľnosti, odporúčame sledovať jednotlivé update zasiahnutého softvéru a po vydaní príslušnej aktualizácie ihneď túto na zasiahnuté zariadenia nainštalovať.

Zdroje

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170726-aniacp

NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

SECURITY BULLETIN

Týždeň 26. 07. 2017 – 01. 08. 2017

No: B20170801-03V

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

Identifikátor

Microsoft Office Outlook Memory Corruption Vulnerability

Popis

V Microsoft Outlook bola zistená existencia vzdialeného spustenia kódu (Remote code execution) a to na základe funkcie, akou program analyzuje špeciálne vytvorené e-mailové správy. Útočník, ktorý úspešne zneužil túto zraniteľnosť, by mohol prevziať kontrolu nad postihnutým systémom. Útočník potom môže inštalovať programy, zobrazovať, meniť alebo mazať údaje alebo vytvoriť nové účty s plnými používateľskými právami.

Využitie tejto zraniteľnosti vyžaduje, aby používateľ otvoril špeciálne vytvorený súbor s príslušnou verziou programu Microsoft Outlook. V scenári útoku by mohol útočník zneužiť túto chybu odoslaním špeciálne vytvoreného súboru používateľovi a potom tohto presvedčiť, aby otvoril súbor.

Aktualizácia zabezpečenia rieši túto zraniteľnosť opravou spôsobu, akým program Microsoft Outlook analyzuje špeciálne vytvorené e-mailové správy.

CVE

CVE-2017-8663

Zasiahnuté systémy

Microsoft Outlook a Microsoft Office Click-to-run vo verziách 2010 až 2016 (32 aj 64-bitové)

Následky

Vzdialené spustenie škodlivého kódu

Odporúčania

Odporúčame bez meškania vykonať aktualizáciu Microsoft Outlook a Microsoft Office Click-to-run softvéru na najnovšiu verziu, nakoľko Microsoft vydal opravu tejto zraniteľnosti.

Zdroje

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8663

NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

SECURITY BULLETIN

Týždeň 26. 07. 2017 – 01. 08. 2017

No: B20170801-04V

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

Identifikátor

Microsoft Office Outlook Information Disclosure Vulnerability

Popis

Information disclosure zraniteľnosť sa vyskytuje, ak program Microsoft Office nesprávne sprístupňuje obsah svojej pamäte. Útočník, ktorý túto chybu zneužil, by mohol tieto informácie použiť na útok na počítač alebo dáta používateľa.
Na zneužitie tejto zraniteľnosti útočník vytvorí špeciálny súbor a následne môže presvedčiť užívateľa zasiahnutého systému, aby ho otvoril. Útočník musí poznať miesto adresy pamäte, kde bol objekt vytvorený.
Aktualizácia rieši túto zraniteľnosť zmenou spôsobu, akým niektoré funkcie spracovávajú objekty v pamäti.

CVE

CVE-2017-8572

Zasiahnuté systémy

Microsoft Outlook a Microsoft Office Click-to-run vo verziách 2010 až 2016 (32 aj 64-bitové)

Následky

Neoprávnený prístup k systémom

Odporúčania

Odporúčame bez meškania vykonať aktualizáciu Microsoft Outlook a Microsoft Offiece Click-to-run softvéru na najnovšiu verziu, nakoľko Microsoft vydal opravu tejto zraniteľnosti.

Zdroje

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8572

NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

SECURITY BULLETIN

Týždeň 26. 07. 2017 – 01. 08. 2017

No: B20170801-05V

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

Identifikátor

Joomla! - Core - Installer: Lack of Ownership Verification Vulnerability

Popis

Inštalátor aplikácie CMS neobsahoval proces na overenie vlastníctva používateľov webového priestoru, čo potenciálne umožňuje používateľom získať kontrolu.

CVE

CVE-2017-11364

Zasiahnuté systémy

Joomla! CMS versions 1.0.0 through 3.7.3

Následky

Neoprávnené získanie kontroly nad systémom

Odporúčania

Odporúčame bez meškania vykonať aktualizáciu CMS Joomla!

Zdroje

https://developer.joomla.org/security-centre/700-20170704-core-installer-lack-of-ownership-verification

NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

SECURITY BULLETIN

Týždeň 26. 07. 2017 – 01. 08. 2017

No: B20170801-06V

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

Identifikátor
Joomla! - Core - XSS Vulnerability

Popis
Nedostatočné filtrovanie potenciálne škodlivých HTML tagov vedie k zraniteľnosti XSS v rôznych komponentoch.

CVE
CVE-2017-11612

Zasiahnuté systémy
Joomla! CMS versions 1.5.0 through 3.7.3

Následky
XSS útok

Odporúčania
Odporúčame bez meškania vykonať aktualizáciu CMS Joomla!

Zdroje
https://developer.joomla.org/security-centre/701-20170704-core-installer-lack-of-ownership-verification