BEZPEČNOSTNÝ BULLETIN

Týždeň 15. 08. 2018 – 21. 08. 2018

OBSAH BEZPEČNOSTNÉHO BULLETINU

Národný bezpečnostný úrad
Budatínska 30
851 06 Bratislava

Mail: *sk-cert@nbu.gov.sk*
Mobil: *+421 903 993 706*
Tel: *+421 2 6869 2915*

SK-CERT
Naša značka:
02049/2018/TS/OKB-114

BEZPEČNOSTNÝ BULLETIN

Týždeň 15. 08. 2018 – 21. 08. 2018

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.8**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Multiple Vulnerabilities in PHP Could Allow for Arbitrary Code Execution

Popis

Vývojári skriptovacieho jazyka PHP vydali bezpečnostnú aktualizáciu, ktorá rieši viacero bezpečnostných zraniteľností.
Bližšie nešpecifikované zraniteľnosti by vzdialený neautentifikovaný útočník mohol zneužiť na vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

20.08.2018

CVE

-

Zasiahnuté systémy

PHP 7.2 verzie staršie ako 7.2.9
PHP 7.1 verzie staršie ako 7.1.21

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-php-could-allow-for-arbitrary-code-execution_2018-092/

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.6**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Cisco Releases Security Updates

Popis

Spoločnosť Cisco vydala bezpečnostné aktualizácie, ktoré opravujú bezpečnostné zraniteľnosti vo viacerých produktoch.

Najzávažnejšia je bezpečnostná zraniteľnosť v produkte **Cisco AsyncOS Software**, ktorá sa nachádza v komponente Web Proxy a vzdialený neautentifikovaný útočník by ju prostredníctvom vytvorenia veľkého množstva TCP spojení mohol zneužiť na zahltenie pamäte zariadenia a následné znneprístupnenie služby.

Zraniteľnosť v produktoch **Cisco Unified Communications Manager IM & Presence Service** a **Cisco TelePresence Video Communication Server (VCS) and Expressway** spočíva v nedostatočnom overovaní používateľských vstupov v komponente XCP Router a vzdialený neautentifikovaný útočník by ju prostredníctvom podvrhnutia špeciálne vytvorených IP paketov na TCP port 7400 mohol zneužiť na znneprístupnenie služby.

Zraniteľnosť v produkte **Cisco Unified Communications Domain Manager Software** spočíva v nedostatočnom overovaní používateľských vstupov a vzdialený neautentifikovaný útočník by ju mohol zneužiť na realizáciu XSS (Cross-Site Scripting) útokov a vykonanie škodlivého kódu.

Zraniteľnosť v produktoch **Cisco Small Business 100/300 Series Wireless Access Points** spočívajú v implementačných chybách vo funkcionalite EAPOL a neautentifikovaný útočník nachádzajúci sa v rovnakom sieťovom segmente by ich mohol zneužiť na znneprístupnenie služby.

Zraniteľnosť vo webovom manažmentovom rozhraní **Cisco Registered Envelope Service** spočíva v nedostatočnom overovaní používateľských vstupov a vzdialený neautentifikovaný útočník by ju mohol zneužiť na realizáciu XSS (Cross-Site Scripting) útoku, vykonanie škodlivého kódu vo webovom prehliadači a získanie prístupu k údajom uloženým v cookies, vrátane autentifikačných údajov.

Zraniteľnosť v produkte **Cisco Digital Network Architecture Center** spočíva v nedostatočnom overovaní používateľských vstupov v rámci CronJob Scheduler API a vzdialený neautentifikovaný útočník by ju mohol zneužiť na vykonanie škodlivého kódu.

Zraniteľnosť v produkte **Cisco ASR 9000 Series Aggregation Services Router Software** sa nachádza v komponente Local Packet Transport Services a vzdialený neautentifikovaný útočník by ju mohol zneužiť na znneprístupnenie služby.

Dátum prvého zverejnenia varovania

15.08.2018

CVE

CVE-2018-0367, CVE-2018-0386, CVE-2018-0409, CVE-2018-0410, CVE-2018-0412, CVE-2018-0415, CVE-2018-0418, CVE-2018-0427, CVE-2018-0428

Zasiahnuté systémy
Cisco Web Security Appliance Cisco AsyncOS Software Releases 9.1, 10.1, 10.5 a 11.0 pre Cisco Web Security Appliance Cisco Unified Communications Manager IM & Presence Service Cisco TelePresence Video Communication Server (VCS) and Expressway Cisco Unified Communications Domain Manager Software Cisco Small Business 100 Series Wireless Access Points Cisco Small Business 300 Series Wireless Access Points Cisco Registered Envelope Service Cisco Digital Network Architecture Center Cisco ASR 9000 Series Aggregation Services Router Software

Následky
Vykonanie škodlivého kódu, Zneprístupnenie služby, Eskalácia privilégií

Odporúčania
Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180815-wsa-dos https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180815-wsa-escalation https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180815-ucmimps-dos https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180815-cucdm-xss https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180815-sb-wap-encrypt https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180815-csb-wap-dos https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180815-res-xss https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180815-dna-injection https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180815-asr-ptp-dos

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.2**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

PowerLogic PM5560 Vulnerability

Popis

Spoločnosť Schneider Electric vydala bezpečnostnú aktualizáciu, ktorá opravuje bezpečnostnú zraniteľnosť v produkte PowerLogic PM5560.
Zraniteľnosť v zabudovanom webovom serveri spočíva v nedostatočnom overovaní používateľských vstupov a vzdialený neautentifikovaný útočník by ju mohol zneužiť na realizáciu XSS (Cross-Site Scripting) útoku a vykonanie škodlivého JavaScript kódu vo webovom prehliadači.

Dátum prvého zverejnenia varovania

16.08.2018

CVE

CVE-2018-7795

Zasiahnuté systémy

PM5560 verzie firmvéru staršie ako 2.5.4

Následky

Vykonanie škodlivého kódu, Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://download.schneider-electric.com/files?p_enDocType=Technical+leaflet&p_File_Name=SEVD-2018-228-01-PowerLogic+PM5560.pdf

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.0**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Samba Releases Security Updates

Popis

Vývojári softvéru Samba vydali aktualizácie svojho produktu, ktoré opravujú viacero bezpečnostných zraniteľností.
Najvážnejšia bezpečnostná zraniteľnosť sa nachádza v komponente LDAP server a autentifikovaný útočník nachádzajúci sa v rovnakom sieťovom segmente by ju mohol zneužiť na neoprávnený prístup k citlivým údajom a vykonanie zmien v systéme.
Zraniteľnosť v komponente libsmbclient spočíva v nedostatočnom overovaní používateľských vstupov a autentifikovaný útočník nachádzajúci sa v rovnakom sieťovom segmente by ju mohol zneužiť na poškodenie pamäte a následné zneprístupnenie služieb.
Zraniteľnosť v komponente NTML (NT Lan Manager) by vzdialený neautentifikovaný útočník mohol zneužiť na obídenie mechanizmov autentifikácie a získať neoprávnený prístup do systému.
Ostatné zraniteľnosti spočívajú v implementačných chybách v komponentoch Samba Active Directory Domain Controller a DRSUAPI RPC Service a neautentifikovaný útočník v rovnakom sieťovom segmente by ich mohol zneužiť na zneprístupnenie služby.

Dátum prvého zverejnenia varovania

14.08.2018

CVE

CVE-2018-10858, CVE-2018-10918, CVE-2018-10919, CVE-2018-1139, CVE-2018-1140

Zasiahnuté systémy

Samba verzie 3.2.0 až 4.8.3 (CVE-2018-10858)
Samba verzie 4.7.0 a novšie (CVE-2018-10918)
Samba verzie 4.0.0 a novšie (CVE-2018-10919)
Samba verzie 4.7.0 až 4.8.3 (CVE-2018-1139)
Samba verzie 4.8.0 a novšie (CVE-2018-1140)

Následky

Zneprístupnenie služby, Neoprávnená zmena v systéme, Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje
https://www.samba.org/samba/security/CVE-2018-1140.html
https://www.samba.org/samba/security/CVE-2018-1139.html
https://www.samba.org/samba/security/CVE-2018-10919.html
https://www.samba.org/samba/security/CVE-2018-10918.html
https://www.samba.org/samba/security/CVE-2018-10858.html

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.8**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

F5 BIG-IP Multiple Vulnerabilities

Popis

Spoločnosť F5 vydala bezpečnostné aktualizácie na svoj produkt BIG-IP, ktoré opravujú viacero bezpečnostných zraniteľností.
Zraniteľnosti spočívajú v nesprávnej konfigurácii komponentov svpn, policyserver a Windows Logon Integration a lokálny autentifikovaný útočník by ich mohol prostredníctvom podvrhnutia špeciálne vytvorených požiadaviek zneužiť na neoprávnený prístup k citlivým údajom, ich manipuláciu a následnú eskaláciu privilégií.

Dátum prvého zverejnenia varovania

17.08.2018 (posledná aktualizácia 20.08.2018)

CVE

CVE-2018-5546, CVE-2018-5547

Zasiahnuté systémy

BIG-IP

Následky

Eskalácia privilégií, Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://support.f5.com/csp/article/K10015187
https://support.f5.com/csp/article/K54431371
https://exchange.xforce.ibmcloud.com/vulnerabilities/148502
https://exchange.xforce.ibmcloud.com/vulnerabilities/148503

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.5**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Linux Kernel IP Fragment Reassembly Denial of Service Vulnerability

Popis

Vývojári linuxového jadra vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť spočívajúcu v nesprávnej implementácii spracovania fragmentovaných IPv4 a IPv6 paketov.
Uvedenú zraniteľnosť by vzdialený neautentifikovaný útočník mohol prostredníctvom podvrhnutia špeciálne vytvorenej sekvencie fragmentovaných IP paketov zneužiť na zahltenie CPU a následné zneprístupnenie služby.

Dátum prvého zverejnenia varovania

14.08.2018 (posledná aktualizácia 20.08.2018)

CVE

CVE-2018-5391

Zasiahnuté systémy

Linux kernel verzie 3.9 a vyššie

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.kb.cert.org/vuls/id/641765
https://tools.cisco.com/security/center/viewAlert.x?alertId=58766

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.3**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Trend Micro Control Manager Multiple Vulnerabilities

Popis

Spoločnosť Trend Micro vydala bezpečnostné aktualizácie, ktoré opravujú viacero bezpečnostných zraniteľností v produkte Control Manager.
Najzávažnejšia zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a vzdialený útočník by ju prostredníctvom podvrhnutia špeciálne vytvorených URL obsahujúcich /../ sekvencie mohol zneužiť na vykonanie škodlivého kódu.
Ostatné zraniteľnosti by vzdialený neautentifikovaný útočník mohol zneužiť na realizáciu SSRF (Server-Side Request Forgery) útokov a lokálny neautentifikovaný útočník na zneprístupnenie služby.

Dátum prvého zverejnenia varovania

15.08.2018

CVE

CVE-2018-10510, CVE-2018-10511, CVE-2018-10512

Zasiahnuté systémy

Trend Micro Control Manger verzie 6.0, 7.0

Následky

Vykonanie škodlivého kódu, zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://success.trendmicro.com/solution/1120112
https://exchange.xforce.ibmcloud.com/vulnerabilities/148455
https://exchange.xforce.ibmcloud.com/vulnerabilities/148456
https://exchange.xforce.ibmcloud.com/vulnerabilities/148457

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre: 6.1**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Philips PageWriter Cardiographs Multiple Vulnerabilities

Popis

EKG zariadenia série PageWriter TC10, TC20, TC30, TC50, TC70 od spoločnosti Philips obsahujú viacero bezpečnostných zraniteľností.
Najzávažnejšia zraniteľnosť spočíva v existencii zabudovaného používateľského účtu s predvoleným heslom a umožňujú neautentifikovanému útočníkovi s fyzickým prístupom k zariadeniu eskalovať svoje privilégiá a vykonávať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

16.08.2018

CVE

CVE-2018-10626, CVE-2018-14801

Zasiahnuté systémy

EKG PageWriter TC10, TC20, TC30, TC50, TC70 všetky verzie staršie ako Máj 2018

Následky

Eskalácia privilégií, Neoprávnená zmena v systéme

Odporúčania

Na uvedenú zraniteľnosť v súčasnosti nie sú dostupné aktualizácie a spoločnosť Phillips plánuje vydať aktualizáciu až v priebehu roku 2019. Administrátorom a používateľom odporúčame limitovať fyzický prístup k zariadeniam len na oprávnené osoby.

Zdroje

https://ics-cert.us-cert.gov/advisories/ICSMA-18-228-01
https://www.usa.philips.com/healthcare/about/customer-support/product-security