BEZPEČNOSTNÝ BULLETIN

Týždeň 11. 07. 2018 – 17. 07. 2018

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Cisco IP Phone 6800, 7800, and 8800 Series with Multiplatform Firmware Web UI Command Injection Vulnerability	Vysoká	**8.8**
02.	VLC Media Player Arbitrary Code Execution Vulnerability	Vysoká	**8.8**
03.	Antenna House Multiple Vulnerabilities	Vysoká	**8.8**
04.	Cisco StarOS IPv4 Fragmentation Denial of Service Vulnerability	Vysoká	**8.6**
05.	Apache Spark and Cassandra Multiple Vulnerabilities	Vysoká	**8.4**
06.	Schweitzer Engineering Laboratories Compass and AcSELerator Architect Vulnerabilities	Vysoká	**8.2**
07.	Siemens EN100 Ethernet Communication Module and SIPROTEC 5 Relay DoS Vulnerability	Vysoká	**7.5**
08.	cURL Heap-Based Buffer Overflow Vulnerability	Vysoká	**7.5**
09.	Clam AntiVirus Denial of Service Vulnerability	Vysoká	**7.5**
10.	Micro Focus Fortify Software Security Center Vulnerability	Vysoká	**7.3**
11.	QNAP Qcenter Virtual Appliance Multiple Vulnerabilities	Vysoká	**7.2**
12.	VMware Tools HGFS Vulnerability	Vysoká	**7.0**
13.	ISC Kea 1.4.0 Failure to Release Memory	Stredná	**6.5**
14.	ELO Enterprise and Professional SQL Injection Vulnerability	Stredná	**6.5**
15.	SAP Security Patch - July 2018	Stredná	**6.4**
16.	Multiple Vulnerabilities in WAGO e!DISPLAY Devices	Stredná	**6.3**
17.	PAN-OS Management Web Interface Information Disclosure Vulnerability	Stredná	**4.9**

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-092

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

Identifikátor

Cisco IP Phone 6800, 7800, and 8800 Series with Multiplatform Firmware Web UI Command Injection Vulnerability

Popis

Spoločnosť Cisco vydala varovanie na bezpečnostné zraniteľnosti vo webovom rozhraní produktov Cisco IP Phone 6800, 7800 a 8800.
Bezpečnostná zraniteľnosť je spôsobená nedostatočným overovaním používateľských vstupov a vzdialený autentifikovaný útočník by ju mohol zneužiť na vykonanie škodlivého kódu.

Dátum prvého zverejnenia varovania

11.07.2018 (posledná aktualizácia 12.07.2018)

CVE

CVE-2018-0341

Zasiahnuté systémy

Cisco IP Phone 6800, 7800, 8800 s Multiplatform Firmware verzie staršie ako 11.2(1)

Následky

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

Odporúčania

Na uvedenú zraniteľnosť v súčasnosti nie sú dostupné aktualizácie. Spoločnosť Cisco na uvedenú zraniteľnosť plánuje vydať bezpečnostné záplaty v auguste 2018. Administrátorom odporúčame sledovať stránky výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180711-phone-webui-inject

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

Identifikátor

VLC Media Player Arbitrary Code Execution Vulnerability

Popis

Vývojári multimediálneho prehrávača VLC Media Player vydali bezpečnostnú aktualizáciu, ktorá opravuje bezpečnostnú zraniteľnosť v časti zodpovednej za spracovanie MKV súborov. Bezpečnostnú zraniteľnosť by vzdialený neautentifikovaný útočník prostredníctvom podvrhnutia špeciálne vytvorených MKV súborov mohol zneužiť na vykonanie škodlivého kódu v kontexte prihláseného používateľa.
Na uvedenú zraniteľnosť je voľne dostupný exploit.

Dátum prvého zverejnenia varovania

09.07.2018 (posledná aktualizácia 11.07.2018)

CVE

CVE-2018-11529

Zasiahnuté systémy

VLC Media Player verzie 2.2.8

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

http://seclists.org/fulldisclosure/2018/Jul/28

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

Identifikátor

Antenna House Multiple Vulnerabilities

Popis

Vývojári konvertora Antenna House Office Server Document Converter vydali bezpečnostnú aktualizáciu, ktorá opravuje viacero bezpečnostných zraniteľností.
Bezpečnostné zraniteľnosti by vzdialený neautentifikovaný útočník prostredníctvom podvrhnutia špeciálne vytvorených .doc a .ppt súborov mohol zneužiť na vykonanie škodlivého kódu v kontexte prihláseného používateľa.

Dátum prvého zverejnenia varovania

10.07.2018

CVE

CVE-2018-3929, CVE-2018-3930, CVE-2018-3931, CVE-2018-3932, CVE-2018-3933, CVE-2018-3936

Zasiahnuté systémy

Antenna House Office Server Document Converter verzia V6.1 Pro MR2 pre Linux64

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://blog.talosintelligence.com/2018/07/vuln-spotlight-antenna.html

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

Identifikátor

Cisco StarOS IPv4 Fragmentation Denial of Service Vulnerability

Popis

Spoločnosť Cisco vydala bezpečnostnú aktualizáciu na svoj produkt Cisco StarOS, ktorá opravuje bezpečnostnú zraniteľnosť spočívajúcu v nesprávnom spracovaní fragmentovaných IPv4 paketov.
Bezpečnostnú zraniteľnosť by vzdialený neautentifikovaný útočník prostredníctvom podvrhnutia špeciálne upravených IPv4 paketov mohol zneužiť na reštartovanie *npusim* procesov a tým spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

11.07.2018

CVE

CVE-2018-0369

Zasiahnuté systémy

Cisco Virtualized Packet Core-Single Instance (VPC-SI)
Cisco Virtualized Packet Core-Distributed Instance (VPC-DI)
Cisco Ultra Packet Core (UPC)

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180711-staros-dos

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.4**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Apache Spark and Cassandra Multiple Vulnerabilities

Popis

Spoločnosť Apache vydala bezpečnostné aktualizácie, ktoré opravujú viacero bezpečnostných zraniteľností v produktoch Apache Spark a Apache Cassandra.

Najzávažnejšia zraniteľnosť v Apache Spark spočíva v bližšie nešpecifikovanej implementačnej chybe v komponentoch *PySpark* a *SparkR* a lokálny neautentifikovaný útočník by ju mohol zneužiť na eskaláciu privilégií.

Druhá zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a vzdialený neautentifikovaný útočník by ju mohol zneužiť na realizáciu XSS (Cross-Site Scripting) útoku, vykonanie škodlivého kódu v prehliadači a získanie prístupu k údajom uloženým v cookies, vrátane autentifikačných údajov.

Zraniteľnosť v produkte Apache Cassandra by vzdialený neautentifikovaný útočník prostredníctvom podvrhnutia škodlivého JAVA kódu cez JMX/RMI (Java Management Extensions/Remote Method Invocation) rozhranie mohol zneužiť na vykonanie škodlivého kódu. Na uvedenú zraniteľnosť je voľne dostupný exploit.

Dátum prvého zverejnenia varovania

11.07.2018

CVE

CVE-2018-1334, CVE-2018-8024

Zasiahnuté systémy

Apache Spark verzie 2.1.2 a staršie, 2.2.0 až 2.2.1 a 2.3.0
Apache Cassandra verzie 3.8 až 3.11.1

Následky

Vykonanie škodlivého kódu, Eskalácia privilégií, Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov, aplikovať firewallové pravidlá a limitovať prístup k zasiahnutým systémom zavedením zoznamu pre riadenie prístupov (ACL).

Zdroje

https://spark.apache.org/security.html
https://exchange.xforce.ibmcloud.com/vulnerabilities/146303
https://exchange.xforce.ibmcloud.com/vulnerabilities/146304
https://tools.cisco.com/security/center/viewAlert.x?alertId=58318

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

Identifikátor

Schweitzer Engineering Laboratories Compass and AcSELerator Architect Vulnerabilities

Popis

Spoločnosť Schweitzer Engineering Laboratories vydala bezpečnostné aktualizácie, ktoré opravujú viacero zraniteľností v produktoch Compass a AcSELerator Architect.
Bezpečnostná zraniteľnosť v produkte Compass spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a lokálny autentifikovaný útočník by ju mohol zneužiť na eskaláciu privilégií a vykonanie škodlivého kódu.
Bezpečnostná zraniteľnosť v komponente AcSELerator Architect XML parser spočíva v nedostatočnom overovaní používateľských vstupov a vzdialený neautentifikovaný útočník by ju prostredníctvom podvrhnutia špeciálne vytvoreného XML súboru mohol zneužiť na realizáciu XXE (XML External Entity) útoku a následné získanie prístupu k citlivým údajom alebo zneprístupnenie služby.

Dátum prvého zverejnenia varovania

10.07.2018

CVE

CVE-2018-10604, CVE-2018-10600, CVE-2018-10608

Zasiahnuté systémy

SEL Compass verzia 3.0.5.1 a staršie
SEL AcSELerator Architect verzia 2.2.24.0 a staršie

Následky

Vykonanie škodlivého kódu, Eskalácia privilégií, Zneprístupnenie služby, Neoprávnený prístup k citlivým údajom, Neoprávnená zmena v systéme

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://applied-risk.com/application/files/9315/3129/8127/Applied_Risk_Schweitzer_Engineering_Laboratories_Compass_3.0.5.1_Insecure_File_Permissions_Privilege_Escalation_Vulnerability.pdf
https://applied-risk.com/application/files/1515/3129/8114/Applied_Risk_Schweitzer_Engineering_Laboratories_AcSELerator_Architect_2.2.24.0_Multiple_Vulnerabilities.pdf
https://ics-cert.us-cert.gov/advisories/ICSA-18-191-02
https://www.securityweek.com/power-grid-protection-firm-sel-patches-severe-software-flaws

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

Identifikátor

Siemens EN100 Ethernet Communication Module and SIPROTEC 5 Relay DoS Vulnerability

Popis

Spoločnosť Siemens vydala varovanie a bezpečnostné aktualizácie, ktoré opravujú viacero bezpečnostných zraniteľností v ethernetových komunikačných moduloch EN100 a SIPROTEC 5 relé.
Bližšie nešpecifikované bezpečnostné zraniteľnosti by vzdialený neautentifikovaný útočník prostredníctvom podvrhnutia špeciálne vytvorených paketov cez port 102/tcp mohol zneužiť na zneprístupnenie služby. Zraniteľnosti je možné zneužiť len v prípade, že je na zasiahnutých zariadeniach aktivovaná komunikácia prostredníctvom IEC 61850-MMS.

Dátum prvého zverejnenia varovania

11.07.2018

CVE

CVE-2018-11451, CVE-2018-11452

Zasiahnuté systémy

EN100 firmware variant IEC 61850 verzie staršie ako 4.33
EN100 firmware variant PROFINET všetky verzie
EN100 firmware variant Modbus TCP všetky verzie
EN100 firmware variant DNP3 TCP všetky verzie
SIPROTEC 5 s CPU variant CP100 a CP300 verzie staršie ako 7.80
SIPROTEC 5 s CPU variant CP200 všetky verzie

Následky

Zneprístupnenie služby

Odporúčania

Spoločnosť Siemens pre produkty EN100 firmware variant IEC 61850 a SIPROTEC 5 s CPU variant CP100 a CP300 vydala bezpečnostné aktualizácie a pracuje na aktualizáciách pre ostatné zasiahnuté produkty.
Administrátorom odporúčame aplikovať dostupné aktualizácie, zavedením firewallových pravidiel blokovať prístup k zariadeniam prostredníctvom portu 102/tcp a sledovať stránky výrobcu na dostupnosť aktualizácií pre zvyšné verzie produktov zasiahnutých uvedenými zraniteľnosťami.

Zdroje

https://cert-portal.siemens.com/productcert/pdf/ssa-635129.pdf

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

Identifikátor

cURL Heap-Based Buffer Overflow Vulnerability

Popis

Vývojári produktu cURL vydali bezpečnostnú aktualizáciu, ktorá opravuje bezpečnostnú zraniteľnosť vo funkcii *Curl_smtp_escape_eob* v rámci *lib/smtp.c*.
Uvedenú zraniteľnosť by vzdialený neautentifikovaný útočník prostredníctvom podvrhnutia špeciálneho curl príkazu na odoslanie dát prostredníctvom SMTP mohol zneužiť na vyvolanie pretečenia zásobníka a následné vykonanie škodlivého kódu alebo zneprístupnenie služby.
Na uvedenú zraniteľnosť je voľne dostupný PoC (Proof of Concept) kód.

Dátum prvého zverejnenia varovania

12.07.2018

CVE

CVE-2018-0500

Zasiahnuté systémy

curl verzie 7.54.1 až 7.60.0

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://curl.haxx.se/docs/adv_2018-70a2.html
https://tools.cisco.com/security/center/viewAlert.x?alertId=58430

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

Identifikátor

Clam AntiVirus Denial of Service Vulnerability

Popis

Vývojári antivírusového programu ClamAV vydali bezpečnostnú aktualizáciu, ktorá opravuje bezpečnostnú zraniteľnosť nachádzajúcu sa vo funkcii *parsehwp3_paragraph()* v *libclamav/hwp.c*.
Bezpečnostnú zraniteľnosť by vzdialený neautentifikovaný útočník prostredníctvom podvrhnutia špeciálne vytvoreného HWP (Hangul Word Processor) súboru mohol zneužiť na vyvolanie nekonečného cyklu a následné zneprístupnenie služby.

Dátum prvého zverejnenia varovania

12.07.2018

CVE

CVE-2018-0360

Zasiahnuté systémy

Clam AntiVirus verzie staršie ako 0.100.1

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://secuniaresearch.flexera.com/secunia_research/2018-12

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

Identifikátor

Micro Focus Fortify Software Security Center Vulnerability

Popis

Spoločnosť Micro Focus vydala bezpečnostnú aktualizáciu pre svoj produkt Fortify Software Security Center, ktorá opravuje bezpečnostnú zraniteľnosť umožňujúcu realizáciu XXE (XML External Entity) útokov.
Bezpečnostnú zraniteľnosť by vzdialený neautentifikovaný útočník prostredníctvom podvrhnutia špeciálne vytvoreného XML DTD (Document Type Declarations) údajov mohol zneužiť na neoprávnený prístup k súborom uloženým na serveri alebo na realizáciu SSRF (Server-Side Request Forgery) útokov.

Dátum prvého zverejnenia varovania

12.07.2018

CVE

CVE-2018-12463

Zasiahnuté systémy

Fortify Software Security Center (SSC) verzie 17.1, 17.2, 18.1

Následky

Zneprístupnenie služby, Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://softwaresupport.softwaregrp.com/document/-/facetsearch/document/KM03201563
https://exchange.xforce.ibmcloud.com/vulnerabilities/146301
https://www.securitytracker.com/id/1041286

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.2**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

QNAP Qcenter Virtual Appliance Multiple Vulnerabilities

Popis

Spoločnosť QNAP vydala bezpečnostnú aktualizáciu, ktorá opravuje viacero bezpečnostných zraniteľností v produkte QNAP Qcenter Virtual Appliance.
Bezpečnostné zraniteľnosti spočívajúce v implementačnej chybe v API a komponentoch zodpovedných za zmenu hesla, dátumu, sieťovej a SSH konfigurácie by vzdialený autentifikovaný útočník prostredníctvom podvrhnutia špeciálne vytvorených požiadaviek mohol zneužiť na eskaláciu privilégií alebo vykonanie škodlivého kódu s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

11.07.2018

CVE

CVE-2018-0706, CVE-2018-0707, CVE-2018-0708, CVE-2018-0709, CVE-2018-0710

Zasiahnuté systémy

Qcenter Virtual Appliance verzie 1.7.1063 a staršie

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.qnap.com/en-us/security-advisory/nas-201807-10
https://www.coresecurity.com/advisories/qnap-qcenter-virtual-appliance-multiple-vulnerabilities

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.0**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

VMware Tools HGFS Vulnerability

Popis

Spoločnosť VMware vydala bezpečnostnú aktualizáciu, ktorá opravuje bezpečnostnú zraniteľnosť v produkte VMware Tools.
Zraniteľnosť sa nachádza v HGFS (Host-Guest File System) drivery a lokálny autentifikovaný útočník by ju mohol zneužiť na eskaláciu privilégií alebo neoprávnený prístup k citlivým údajom v bežiacom VM (Virtual Machine).
Uvedenú zraniteľnosť je možné zneužiť len v prípade, že je aktivovaná funkcia zdieľania súborov.

Dátum prvého zverejnenia varovania

13.07.2018

CVE

CVE-2018-6969

Zasiahnuté systémy

VMware Tools verzie staršie ako 10.3.0

Následky

Eskalácia privilégií, Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.vmware.com/security/advisories/VMSA-2018-0017.html
https://tools.cisco.com/security/center/viewAlert.x?alertId=58434

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre: 6.5**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

ISC Kea 1.4.0 Failure to Release Memory

Popis

Vývojári DHCP servera Kea vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť v komponentoch *query4* a *query6*.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii mechanizmov správy pamäte a umožňuje vzdialenému útočníkovi nachádzajúcemu sa v rovnakej podsieti prostredníctvom zasielania veľkého množstva paketov spôsobiť zaplnenie pamäte a následné zneprístupnenie služieb.

Dátum prvého zverejnenia varovania

11.07.2018

CVE

CVE-2018-5739

Zasiahnuté systémy

Kea DHCP verzia 1.4.0

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov. Zneužitiu uvedenej zraniteľnosti možno zabrániť pravidelným reštartovaním Kea DHCPv4 a DHCPv6 služieb.

Zdroje

https://kb.isc.org/article/AA-01626

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre: 6.5**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

ELO Enterprise and Professional SQL Injection Vulnerability

Popis

Spoločnosť ELO Digital Office vydala bezpečnostné aktualizácie, ktoré opravujú bezpečnostnú zraniteľnosť v produktoch na správu dokumentov a elektronického obsahu ELO Enterprise a ELO Professional.
Zraniteľnosť v komponente Access Manager by vzdialený neautentifikovaný útočník mohol zneužiť na vykonanie SQL injekcie a následne zobraziť, pridať, upraviť alebo odstrániť údaje uložené v backend databáze.

Dátum prvého zverejnenia varovania

10.07.2018

CVE

CVE-2018-10197

Zasiahnuté systémy

ELO Enterprise verzie 9, 10
ELO Professional verzie 9, 10

Následky

Neoprávnená zmena v systéme

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov. Následne odporúčame preveriť integritu databázy a prístupové logy na prítomnosť pokusov o SQL injekcie.

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/146273
https://packetstormsecurity.com/files/148478

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre: 6.4**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

SAP Security Patch - July 2018

Popis

Spoločnosť SAP vydala bezpečnostné aktualizácie na svoje produkty, ktoré opravujú viacero bezpečnostných zraniteľností.
Najvážnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných opatrení v komponente *WRCK* v SAP R/3 Enterprise Retail a umožňuje vzdialenému autentifikovanému útočníkovi eskalovať svoje privilégiá na napadnutom systéme.

Dátum prvého zverejnenia varovania

10.07.2018

CVE

CVE-2018-2427, CVE-2018-2431, CVE-2018-2432, CVE-2018-2433, CVE-2018-2434, CVE-2018-2435, CVE-2018-2436, CVE-2018-2437, CVE-2018-2438, CVE-2018-2439, CVE-2018-2440

Zasiahnuté systémy

SAP BusinessObjects Business Intelligence (BI Launchpad and Central Management Console) verzie 4.1, 4.2, 4.3
SAP Dynamic Authorization Management (DAM) by NextLabs (Java Policy Controller) verzie 7.7 a 8.5
SAP Internet Graphics Server (IGS) verzie 7.20, 7.20EXT, 7.45, 7.49, 7.53
SAP MaxDB ODBC driver verzie 7.9.09.07
SAP Gateway
SAP BusinessObjects Business Intelligence Suite verzie 4.10, 4.20
SAP Business Objects Enterprise verzie 4.0, 4.1
SAP R/3 Enterprise Retail verzie EHP6

Následky

Vykonanie škodlivého kódu, Zneprístupnenie služby, Eskalácia privilégií, Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=497256000

BEZPEČNOSTNÝ BULLETIN

Týždeň 11. 07. 2018 – 17. 07. 2018

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre: 6.3**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Multiple Vulnerabilities in WAGO e!DISPLAY Devices

Popis

Spoločnosť WAGO Kontakttechnik GmbH & Co. KG vydala bezpečnostnú aktualizáciu firmvéru pre webové panely WAGO e!DISPLAY, ktorá opravuje viacero bezpečnostných zraniteľností.

Najzávažnejšie zraniteľnosti spočívajú v nedostatočnom overovaní prípon súborov nahrávaných prostredníctvom skriptu *receive_upload.php* a nedostatočnej implementácii bezpečnostných mechanizmov. Vzdialený autentifikovaný útočník by ich prostredníctvom špeciálne vytvorených HTTP požiadaviek mohol zneužiť na nahratie a následné vykonanie škodlivého PHP kódu na zasiahnutých systémoch.

Ďalšia zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov v skripte *configtools.php* a vzdialený neautentifikovaný útočník by ju mohol zneužiť na realizáciu XSS (Cross-Site Scirpting) útoku, vykonanie škodlivého kódu vo webovom prehliadači a získanie prístupu k údajom uloženým v cookies, vrátane autentifikačných údajov.

Dátum prvého zverejnenia varovania

11.07.2018

CVE

CVE-2018-12979, CVE-2018-12980, CVE-2018-12981

Zasiahnuté systémy

WAGO e!DISPLAY 7300T - WP 4.3 480x272 PIO1 FW 01 - 01.01.10(01)

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému. Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu firmvéru zasiahnutých zariadení, aplikovať firewallové pravidlá a limitovať prístup k zasiahnutým zariadeniam a ich funkciám zavedením zoznamu pre riadenie prístupov (ACL).

Zdroje

https://www.wago.com/medias/SA-WBM-2018-004.pdf?context=bWFzdGVyfHJvb3R8MjgyNzYwfGFwcGxpY2F0aW9uL3BkZnxoMWUvaDg4LzkzNjE3NTIxOTUxMDIucGRmfDU1NmJkYjEzNDY0ZGU4OWQ1OTMyMjUwNTlmZTI0MzgwNDQ1MDY1YzU3OWRmZDk1NzYzODAwMDI3ODg1NDJlZjU

http://seclists.org/fulldisclosure/2018/Jul/38

https://www.securityweek.com/hackers-can-chain-multiple-flaws-attack-wago-hmi-devices

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-092

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre: 4.9**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

PAN-OS Management Web Interface Information Disclosure Vulnerability

Popis

Spoločnosť Palo Alto Networks vydala bezpečnostnú aktualizáciu, ktorá opravuje bezpečnostnú zraniteľnosť vo webovom manažmentovom rozhraní PAN-OS.
Bezpečnostnú zraniteľnosť by vzdialený autentifikovaný útočník s administrátorskými právami mohol prostredníctvom úpravy HTML kódu manažmentového rozhrania zneužiť na zobrazenie GlobalProtect hesiel lokálnych používateľov v hash-ovanej podobe.

Dátum prvého zverejnenia varovania

09.07.2018

CVE

CVE-2018-9334

Zasiahnuté systémy

PAN-OS verzie staršie ako 6.1.21
PAN-OS verzie staršie ako 7.1.17
PAN-OS verzie staršie ako 8.0.9
PAN-OS verzie staršie ako 8.1.1

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov. Spoločnosť Palo Alto Networks rovnako odporúča limitovať dostupnosť webového manažmentového rozhrania prostredníctvom postupov, ktoré sú dostupné na nasledujúcom odkaze:
https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/getting-started/best-practices-for-securing-administrative-access

Zdroje

http://securityadvisories.paloaltonetworks.com/Home/Detail/124
https://www.securitytracker.com/id/1041243