BEZPEČNOSTNÝ BULLETIN

Týždeň 14. 11. 2018 - 20. 11. 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-191

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

Identifikátor

Google Chrome a Chrome OS zraniteľnosť

Popis

Spoločnosť Google vydala bezpečnostné aktualizácie, ktoré opravujú bezpečnostnú zraniteľnosť v internetovom prehliadači Google Chrome a operačnom systéme Chrome OS.
Bližšie nešpecifikovanú bezpečnostnú zraniteľnosť by vzdialený útočník mohol zneužiť na vykonanie škodlivého kódu v kontexte webového prehliadača a úplné narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

19.11.2018

CVE

CVE-2018-17479

Zasiahnuté systémy

Google Chrome verzie staršie ako 70.0.3538.110
Chrome OS verzie staršie ako 70.0.3538.110 (Platform version: 11021.81.0)

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov. Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.

Zdroje

https://chromereleases.googleblog.com/search/label/Stable%20updates

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

Identifikátor

Zraniteľnosť serverov Lenovo ThinkServer

Popis

Spoločnosť Lenovo vydala bezpečnostné aktualizácie na svoje produkty ThinkServer, ktoré opravujú bezpečnostnú zraniteľnosť vo firmvéri BMC.
Bezpečnostná zraniteľnosť je spôsobená nedostatočným overovaním používateľských vstupov a umožňuje vzdialenému autentifikovanému útočníkovi prostredníctvom zasielania špeciálne upravených požiadaviek vykonať škodlivý kód.

Dátum prvého zverejnenia varovania

15.11.2018

CVE

CVE-2018-9086

Zasiahnuté systémy

Lenovo ThinkServer RD340 verzie staršie ako 64.00
Lenovo ThinkServer RD440 verzie staršie ako 64.00
Lenovo ThinkServer RD640 verzie staršie ako 64.00
Lenovo ThinkServer TD340 verzie staršie ako 60.00

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://support.lenovo.com/sk/en/solutions/len-23836
https://exchange.xforce.ibmcloud.com/vulnerabilities/152994

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

Identifikátor

Zraniteľnosť Lenovo produktov

Popis

Spoločnosť Lenovo vydala bezpečnostné aktualizácie na svoje produkty ThinkServer, IdeaCentre, QITIAN a YANGTIAN, ktoré opravujú bezpečnostnú zraniteľnosť v BIOSe AMI.
Bližšie nešpecifikovaná bezpečnostná zraniteľnosť umožňuje vzdialenému neautentifikovanému útočníkovi vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

15.11.2018

CVE

-

Zasiahnuté systémy

Lenovo IdeaCentre
Lenovo ThinkCentre
Lenovo QITIAN
Lenovo YANGTIAN
Kompletný zoznam zasiahnutých systémov nájdete v odkaze v časti ZDROJE.

Následky

Neoprávnená zmena v systéme

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://support.lenovo.com/sk/en/solutions/len-24239
https://exchange.xforce.ibmcloud.com/vulnerabilities/153023

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

Identifikátor

Zraniteľnosti Siemens SIMATIC Panel a SIMATIC WinCC

Popis

Spoločnosť Siemens vydala bezpečnostné aktualizácie na svoje produkty SIMATIC Panel a SIMATIC WinCC, ktoré opravujú viacero bezpečnostných zraniteľností. Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému neautentifikovanému útočníkovi získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

13.11.2018

CVE

CVE-2018-13812, CVE-2018-13813, CVE-2018-13814

Zasiahnuté systémy

SIMATIC HMI Comfort Panels 4" - 22" verzie staršie ako V15 Update 4
SIMATIC HMI Comfort Outdoor Panels 7" & 15" verzie staršie ako V15 Update 4
SIMATIC HMI KTP Mobile Panels KTP400F, KTP700, KTP700F, KTP900 a KTP900F verzie staršie ako V15 Update 4
SIMATIC WinCC verzie staršie ako V15 Update 4

Následky

Neoprávnený prístup do systému, Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov. Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

https://cert-portal.siemens.com/productcert/pdf/ssa-233109.pdf
https://cert-portal.siemens.com/productcert/pdf/ssa-944083.pdf

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

Identifikátor

Zraniteľnosť Squid SNMP zneprístupnenie služby

Popis

Vývojári proxy servera Squid vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť v SNMP komponente.
Bezpečnostná zraniteľnosť spočíva v nesprávnom spracovaní SNMP paketov a umožňuje vzdialenému neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne upravených SNMP paketov spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

28.11.2018

CVE

CVE-2018-19132

Zasiahnuté systémy

Squid verzie 3.2.0.10 až 3.5.28
Squid verzie 4.x až 4.3

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

http://www.squid-cache.org/Advisories/SQUID-2018_5.txt
https://tools.cisco.com/security/center/viewAlert.x?alertId=59123

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

Identifikátor

Zraniteľnosti v produktoch Adobe

Popis

Spoločnosť Adobe vydala bezpečnostné aktualizácie na svoje produkty Adobe Acrobat a Reader, Flash Player, Photoshop CC, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť sa nachádza v produktoch Acrobat DC a Reader a umožňuje útočníkovi získať prístup k zašifrovaným NTLM heslám. K uvedenej zraniteľnosti je dostupný PoC kód.

Dátum prvého zverejnenia varovania

13.11.2018

CVE

CVE-2018-15978, CVE-2018-15979, CVE-2018-15980

Zasiahnuté systémy

Photoshop CC, verzie staršie ako 19.1.7 / 20.0
Acrobat DC a Reader, verzie staršie ako 2019.008.20081 / 2017.011.30106 / 2015.006.30457
Adobe Flash Player, verzie staršie ako 31.0.0.148

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom zasiahnutých systémov odporúčame bezodkladne nainštalovať bezpečnostné aktualizácie.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.

Zdroje

https://helpx.adobe.com/security/products/photoshop/apsb18-43.html
https://helpx.adobe.com/security/products/acrobat/apsb18-40.html
https://helpx.adobe.com/security/products/flash-player/apsb18-39.html

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 4.7
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Zraniteľnosť Cross-Site Scripting (XSS) v SCALANCE S

Popis

Spoločnosť Siemens vydala bezpečnostné aktualizácie na svoje produkty SCALANCE S, ktoré opravujú bezpečnostnú zraniteľnosť vo webovom rozhraní. Bezpečnostná zraniteľnosť umožňuje vzdialenému útočníkovi pomocou podvrhnutia špeciálne upravených URL adries vykonať škodlivý kód.

Dátum prvého zverejnenia varovania

13.11.2018

CVE

CVE-2018-16555

Zasiahnuté systémy

SCALANCE S602, S612, S623, S627-2M, všetky verzie firmvéru staršie ako V4.0.1.1

Následky

Vykonanie škodlivého kódu

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://cert-portal.siemens.com/productcert/pdf/ssa-242982.pdf