BEZPEČNOSTNÝ BULLETIN

Týždeň 11. 12. 2019 - 17. 12. 2019

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Google Chrome viacero zraniteľností	Vysoká	**8.8**
02.	Omron PLC viacero zraniteľností	Vysoká	**8.6**
03.	Intel produkty viacero zraniteľností	Vysoká	**8.2**
04.	Schneider Electric produkty viacero zraniteľností	Vysoká	**7.8**
05.	Cisco Wireless LAN Controller zraniteľnosť	Vysoká	**7.7**
06.	WordPress bezpečnostné zraniteľnosti	Vysoká	**7.5**
07.	ABB PB610 Panel Builder 600 zraniteľnosti	Vysoká	**7.1**

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:
01380/2019/SK-CERT-294

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

Identifikátor

Google Chrome viacero zraniteľností

Popis

Spoločnosť Google vydala aktualizáciu na svoj internetový prehliadač Google Chrome, ktorá opravuje 51 bezpečnostných zraniteľností.
Najzávažnejšie bezpečnostné zraniteľnosti umožňujú vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upraveného webového obsahu vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

10.12.2019

CVE

CVE-2019-13725, CVE-2019-13726, CVE-2019-13727, CVE-2019-13728, CVE-2019-13729, CVE-2019-13730, CVE-2019-13732, CVE-2019-13734, CVE-2019-13735, CVE-2019-13736, CVE-2019-13737, CVE-2019-13738, CVE-2019-13739, CVE-2019-13740, CVE-2019-13741, CVE-2019-13742, CVE-2019-13743, CVE-2019-13744, CVE-2019-13745, CVE-2019-13746, CVE-2019-13747, CVE-2019-13748, CVE-2019-13749, CVE-2019-13750, CVE-2019-13751, CVE-2019-13752, CVE-2019-13753, CVE-2019-13754, CVE-2019-13755, CVE-2019-13756, CVE-2019-13757, CVE-2019-13758, CVE-2019-13759, CVE-2019-13761, CVE-2019-13762, CVE-2019-13763, CVE-2019-13764

Zasiahnuté systémy

Google Chrome verzie staršie ako 79.0.3945.79

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov. Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.
Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://chromereleases.googleblog.com/2019/12/stable-channel-update-for-desktop.html
https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-google-chrome-could-allow-for-arbitrary-code-execution_2019-129/
https://www.bleepingcomputer.com/news/google/chrome-79-released-with-security-improvements-proactive-tab-freeze-and-more/

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

Identifikátor

Omron PLC viacero zraniteľností

Popis

Spoločnosť Omron informovala o viacerých bezpečnostných zraniteľnostiach vo svojich produktoch Omron PLC.
Najzávažnejšie bezpečnostné zraniteľnosti sú spôsobené nedostatočnou implementáciou bezpečnostných mechanizmov a umožňujú vzdialenému, neautentifikovanému útočníkovi v komponente Teamviewer umožňujú vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup do systému a vykonávať neoprávnené zmeny.

Dátum prvého zverejnenia varovania

06.12.2019

CVE

CVE-2019-13533, CVE-2019-18259, CVE-2019-18261, CVE-2019-18269

Zasiahnuté systémy

Omron PLC CS series
Omron PLC CJ series
Omron PLC NJ series

Následky

Zneprístupnenie služby
Neoprávnený prístup do systému
Neoprávnená zmena v systéme

Odporúčania

Administrátorom odporúčame aplikovať firewallové pravidlá, zablokovať porty FTP 21 a FINS 9600 a limitovať prístup k zasiahnutým zariadeniam a jeho funkciám zavedením zoznamu pre riadenie prístupov (ACL).
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

http://www.omron-cxone.com/security/2019-12-06_PLC_EN.pdf
https://www.us-cert.gov/ics/advisories/icsa-19-346-03
https://www.us-cert.gov/ics/advisories/icsa-19-346-02
https://exchange.xforce.ibmcloud.com/vulnerabilities/173032
https://exchange.xforce.ibmcloud.com/vulnerabilities/173034
https://exchange.xforce.ibmcloud.com/vulnerabilities/173030
https://exchange.xforce.ibmcloud.com/vulnerabilities/173031

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

Identifikátor

Intel produkty viacero zraniteľností

Popis

Spoločnosť Intel vydala bezpečnostné aktualizácie na svoje produkty, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšie zraniteľnosti vo firmvéri Intel NUC a Intel® Network Adapters umožňujú lokálnemu, autentifikovanému útočníkovi eskalovať svoje privilégiá a získať úplnú kontrolu nad systémom.

Dátum prvého zverejnenia varovania

10.12.2019

CVE

CVE-2019-0134, CVE-2019-0159, CVE-2019-11096, CVE-2019-11157, CVE-2019-11165, CVE-2019-14568, CVE-2019-14599, CVE-2019-14603, CVE-2019-14604, CVE-2019-14605, CVE-2019-14607, CVE-2019-14608, CVE-2019-14609, CVE-2019-14610, CVE-2019-14611, CVE-2019-14612

Zasiahnuté systémy

Intel® NUC® Firmware
Intel® RST verzie staršie ako 17.7.0.1006
Intel® Dynamic Platform and Thermal Framework verzia v8.3.10208.5643 a staršie
Intel® Ethernet I218 Adapter driver for Windows* 10 verzie staršie ako 24.1
Intel® Quartus® Prime Pro verzie staršie ako 19.3
Control Center-I
Intel® 6th, 7th, 8th, 9th & 10th Generation Core™ Processors
Intel® Xeon® Processor E3 v5 & v6 and Intel® Xeon® Processor E-2100 & E-2200
Linux Administrative Tools for Intel® Network Adapters verzie staršie ako 24.3.
Intel® FPGA SDK for OpenCL™ verzie staršie ako 19.4
Intel® SCS Platform Discovery Utility všetky verzie

Následky

Eskalácia privilégií
Zneprístupnenie služby
Neoprávnený prístup k citlivým údajom
Neoprávnený prístup do systému

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Produktu Intel® SCS Platform Discovery Utility bola ukončená technická podpora a preto odporúčame jeho odinštalovanie.
Po odstránení zraniteľností, ktoré môžu spôsobiť únik informácií, je dobrou praxou zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00237.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00284.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00289.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00299.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00311.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00253.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00230.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00324.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00323.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00317.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00312.html

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

Identifikátor

Schneider Electric produkty viacero zraniteľností

Popis

Spoločnosť Schneider Electric vydala bezpečnostné aktualizácie na svoje produkty, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť v produkte EcoStruxure Geo SCADA Expert (ClearSCADA) je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi vykonávať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

10.12.2019

CVE

CVE-2018-7794, CVE-2019-13537, CVE-2019-6854, CVE-2019-6855, CVE-2019-6856, CVE-2019-6857

Zasiahnuté systémy

Modicon M580 verzie staršie ako V3.10
Modicon M340 verzie staršie ako V3.20
Modicon Premium verzie staršie ako V3.20
Modicon Quantum verzie staršie ako V3.60
Power SCADA Operation verzie staršie ako 4.15.00
EcoStruxure Geo SCADA Expert (ClearSCADA) verzie staršie ako 2019
EcoStruxure Control Expert verzie staršie ako 14.1

Následky

Zneprístupnenie služby
Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme

Odporúčania

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

Zdroje

https://download.schneider-electric.com/files?p_enDocType=Technical+leaflet&p_File_Name=SEVD-2019-344-02_EcoStruxure_Control_Expert.pdf
https://download.schneider-electric.com/files?p_enDocType=Technical+leaflet&p_File_Name=SEVD-2019-344-05_EcoStruxure_Geo_SCADA_Expert.pdf
https://download.schneider-electric.com/files?p_enDocType=Technical+leaflet&p_File_Name=SEVD-2019-344-04_Power_SCADA_Operation.pdf
https://download.schneider-electric.com/files?p_enDocType=Technical+leaflet&p_File_Name=SEVD-2019-344-01_Modicon_Controllers.pdf

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.7**
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Cisco Wireless LAN Controller zraniteľnosť

Popis

Spoločnosť Cisco vydala bezpečnostnú aktualizáciu na svoj produkt Wireless LAN Controller, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nedostatočným overovaním používateľských vstupov v parsovacom engine HTTP a umožňuje vzdialenému, autentifikovanému útočníkovi spôsobiť zneprístupnenie služieb.

Dátum prvého zverejnenia varovania

06.12.2019

CVE

CVE-2019-15276

Zasiahnuté systémy

Cisco Wireless LAN Controller verzie 8.4 až 8.10

Následky

Zneprístupnenie služieb

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191106-wlc-dos

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

Identifikátor

WordPress bezpečnostné zraniteľnosti

Popis

Vývojári redakčného systému WordPress vydali aktualizáciu svojho produktu, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšie bezpečnostné zraniteľnosti sú spôsobené nedostatočným overovaním používateľských vstupov a umožňujú vzdialenému, neautentifikovanému útočníkovi prostredníctvom XSS útokov získať prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

13.12.2019

CVE

-

Zasiahnuté systémy

WordPress verzie staršie ako 5.3.1

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme

Odporúčania

Odporúčame uistiť sa, či Vaše webové stránky nie sú založené na redakčnom systéme Wordpress v zraniteľnej verzii. V prípade, že áno, zabezpečte aktualizáciu redakčného systému a pluginov.
Po odstránení zraniteľností, ktoré môžu spôsobiť únik informácií, je dobrou praxou zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://wordpress.org/news/2019/12/wordpress-5-3-1-security-and-maintenance-release/

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.1**
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

ABB PB610 Panel Builder 600 zraniteľnosti

Popis

Spoločnosť ABB vydala bezpečnostné aktualizácie na svoj produkt PB610 Panel Builder 600, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia zraniteľnosť v komponente HMIStudio je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi vykonať škodlivý kód.

Dátum prvého zverejnenia varovania

16.12.2019

CVE

CVE-2019-18994, CVE-2019-18995, CVE-2019-18996, CVE-2019-18997

Zasiahnuté systémy

ABB PB610 Panel Builder 600 verzie staršie ako V2.8.0.460

Následky

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

Odporúčania

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

Zdroje

http://search.abb.com/library/Download.aspx?DocumentID=3ADR010466&LanguageCode=en&DocumentPartId=&Action=Launch