BEZPEČNOSTNÝ BULLETIN

Týždeň 13. 11. 2019 - 19. 11. 2019

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Adobe produkty viacero zraniteľností	Vysoká	**8.8**
02.	Google Chrome viacero zraniteľností	Vysoká	**8.8**
03.	WhatsApp zraniteľnosť	Vysoká	**8.8**
04.	ABB Automation Builder and Drive Application Builder zraniteľnosť	Vysoká	**8.6**
05.	Symantec Endpoint Protection zraniteľnosti	Vysoká	**7.8**
06.	Schneider Electric Modicon a Andover Continuum zraniteľnosti	Vysoká	**7.5**
07.	Cisco Adaptive Security Appliance a Firepower Threat Defense zraniteľnosť	Vysoká	**7.2**
08.	Siemens produkty viacero zraniteľností	Vysoká	**7.1**
09.	STMicroelectronics ST33 TPM chip zraniteľnosť	Stredná	**6.8**

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-272

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

Identifikátor

Adobe produkty viacero zraniteľností

Popis

Spoločnosť Adobe vydala aktualizácie na svoje produkty Animate, Brodge, Illustrator a Media Encoder, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšie bezpečnostné zraniteľnosti v Adobe Illustrator umožňujú vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

12.11.2019

CVE

CVE-2019-7960, CVE-2019-7962, CVE-2019-8239, CVE-2019-8240, CVE-2019-8241, CVE-2019-8242, CVE-2019-8243, CVE-2019-8244, CVE-2019-8246, CVE-2019-8247, CVE-2019-8248

Zasiahnuté systémy

Adobe Bridge CC verzie staršie ako 10.0
Adobe Media Encoder verzie staršie ako 14.0
Acrobat Illustrator CC 2019 verzie staršie ako 24.0
Adobe Animate CC 2019 verzie staršie ako 20.0

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
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://helpx.adobe.com/security/products/animate/apsb19-34.html
https://helpx.adobe.com/security/products/illustrator/apsb19-36.html
https://helpx.adobe.com/security/products/media-encoder/apsb19-52.html
https://helpx.adobe.com/security/products/bridge/apsb19-53.html
http://mashviral.com/adobe-patches-critical-bugs-in-illustrator-media-encoder/

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 viacero 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

18.11.2019

CVE

CVE-2019-13720, CVE-2019-13721, CVE-2019-13723, CVE-2019-13724

Zasiahnuté systémy

Google Chrome verzie staršie ako 78.0.3904.108

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/2019/11/stable-channel-update-for-desktop_18.html
https://chromereleases.googleblog.com/2019/10/stable-channel-update-for-desktop_31.html

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

Identifikátor

WhatsApp zraniteľnosť

Popis

Spoločnosť Facebook vydala bezpečnostnú aktualizáciu na svoj produkt WhatsApp, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených MP4 súborov spôsobiť pretečenie zásobníka a vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

14.11.2019

CVE

CVE-2019-11931

Zasiahnuté systémy

WhatsApp for Android verzie staršie ako 2.19.274
WhatsApp for iOS verzie staršie ako 2.19.100
WhatsApp Enterprise Client verzie staršie ako 2.25.3
WhatsApp for Windows Phone verzia 2.18.368 a staršie
WhatsApp Business for Android verzie staršie ako 2.19.104

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
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://www.facebook.com/security/advisories/cve-2019-11931
https://thehackernews.com/2019/11/whatsapp-hacking-vulnerability.html

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

Identifikátor

ABB Automation Builder and Drive Application Builder zraniteľnosť

Popis

Spoločnosť ABB informuje o bezpečnostnej zraniteľnosti vo svojich produktoch Automation Builder a Drive Application Builder.
Bezpečnostná zraniteľnosť umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených EC 61131 knižníc vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

12.11.2019

CVE

CVE-2016-2109, CVE-2016-2177, CVE-2016-2178, CVE-2016-2182, CVE-2016-2183, CVE-2016-6304, CVE-2016-6306, CVE-2017-3737, CVE-2018-0732, CVE-2018-0737, CVE-2018-0739

Zasiahnuté systémy

ABB Drive Application Builder verzie staršie ako 2.3.0
ABB Automation Builder 1.0.0

Následky

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

Odporúčania

Bezpečnostná aktualizácia riešiaca uvedenú zraniteľnosť doposiaľ nebola vydaná.
Odporúčame sledovať stránky výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu. Tiež odporúčame inštalovať EC 61131 knižnice iba z overených zdrojov.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

https://search.abb.com/library/Download.aspx?DocumentID=3ADR010465&LanguageCode=en&DocumentPartId=&Action=Launch

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

Identifikátor

Symantec Endpoint Protection zraniteľnosti

Popis

Spoločnosť Symantec vydala bezpečnostnú aktualizáciu na svoj produkt Endpoint Protection, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť umožňuje lokálnemu, autentifikovanému útočníkovi eskalovať svoje privilégiá na zasiahnutom systéme.

Dátum prvého zverejnenia varovania

14.11.2019

CVE

CVE-2018-18368, CVE-2019-12756, CVE-2019-12757, CVE-2019-12758, CVE-2019-12759, CVE-2019-18372

Zasiahnuté systémy

Symantec Endpoint Protection a Endpoint Protection Manager verzie staršie ako 14.2 RU2
Symantec Endpoint Protection Small Business Edition verzie staršie ako 12.1 RU6 MP10d (12.1.7510.7002)
Symantec Mail Security for MS Exchange verzie staršie ako 7.9.x

Následky

Eskalácia privilégií

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://support.symantec.com/us/en/article.SYMSA1488.html
https://safebreach.com/Post/Symantec-Endpoint-Protection-Self-Defense-Bypass-and-Potential-Usages-CVE-2019-12758

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

Identifikátor

Schneider Electric Modicon a Andover Continuum zraniteľnosti

Popis

Spoločnosť Schneider Electric informovala o bezpečnostných zraniteľnostiach v zariadeniach Modicon a Andover Continuum.
Najzávažnejšia bezpečnostná zraniteľnosť v produktoch Modicon zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

12.11.2019

CVE

CVE-2019-6852, CVE-2019-6853

Zasiahnuté systémy

Modicon M340 CPUs BMX P34x
M340 communication modules BMX NOE 0100, BMX NOE 0110, BMX NOC 0401
Premium CPUs TSX P57x
Premium communication modules TSX ETY x103
Quantum CPUs140 CPU6x
Quantum communication modules 140 NOE 771x1, 140 NOC 78x00, 140 NOC 77101
Andover Continuum models 9680, 5740 and 5720, bCX4040, bCX9640, 9900, 9940, 9924 and 9702

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom zariadení Modicon odporúčame aplikovať firewallové pravidlá a blokovať neautorizovaný prístup na porty 80/HTTP a 21/FTP.
Výrobca ukončil technickú podporu produktov Andover Continuum a vydal nástupnícky produkt EcoStruxure Building Operation.
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.
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-2019-316-02-Modicon_Controllers.pdf
https://download.schneider-electric.com/files?p_enDocType=Technical+leaflet&p_File_Name=SEVD-2019-316-01_Andover_Continuum_Security_Notification.pdf

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

Identifikátor

Cisco Adaptive Security Appliance a Firepower Threat Defense zraniteľnosť

Popis

Spoločnosť Cisco vydala aktualizácie svoje produkty Adaptive Security Appliance a Firepower Threat Defense, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť sa nachádza v komponente Lua interpreter a umožňuje vzdialenému, autentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

12.11.2019

CVE

CVE-2019-15992

Zasiahnuté systémy

Cisco Security Manager
Cisco Adaptive Security Manager
Cisco Firepower Management Center verzie staršie ako VDB Update 329

Následky

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

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých systémov.
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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191112-asa-ftd-lua-rce

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

Identifikátor

Siemens produkty viacero zraniteľností

Popis

Spoločnosť Siemens vydala bezpečnostné aktualizácie na svoje produkty, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť v produktoch Mentor Nucleus a VSTAR umožňuje vzdialenému, neautentifikovanému útočníkovi, nachádzajúcemu sa v rovnakom sieťovom segmente, spôsobiť zneprístupnenie služieb.

Dátum prvého zverejnenia varovania

12.11.2019

CVE

CVE-2019-13927, CVE-2019-13939, CVE-2019-13945

Zasiahnuté systémy

Mentor Nucleus NET
Mentor Nucleus RTOS
Mentor Nucleus ReadyStart verzie staršie ako V2017.02.2 Nucleus NET Patch
Mentor Nucleus Source Code
VSTAR
Desigo PXC00-E.D, PXC50-E.D, PXC100-E.D, PXC200-E.D, PXC00-U, PXC64-U, PXC128-U, PXC22.1-E.D, PXC36-E.D, PXC36.1-E.D verzie staršie ako V6.00.320
Siemens S7-1200 CPU

Následky

Zneprístupnenie služby
Neoprávnená zmena v systéme

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov a vyhnúť sa použitiu DHCP klienta v produkte Nucleus NET.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

https://cert-portal.siemens.com/productcert/txt/ssa-434032.txt
https://cert-portal.siemens.com/productcert/txt/ssa-686531.txt
https://cert-portal.siemens.com/productcert/txt/ssa-898181.txt
https://www.us-cert.gov/ics/advisories/icsa-19-318-03
https://www.us-cert.gov/ics/advisories/icsa-19-318-02
https://www.us-cert.gov/ics/advisories/icsa-19-318-01

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 6.8
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

STMicroelectronics ST33 TPM chip zraniteľnosť

Popis

Bezpečnostní výskumníci informovali o bezpečnostnej zraniteľnosti v STMicroelectronics ST33 TPM chipoch.
Bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom side-channel timing útoku získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

12.11.2019

CVE

CVE-2019-16863

Zasiahnuté systémy

STMicroelectronics ST33TPHF2ESPI TPM chipy vydané pred 12.09.2019

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Na zraniteľných zariadeniach neodporúčame spracovávať citlivé údaje.

Zdroje

http://tpm.fail/
https://www.st.com/content/st_com/en/campaigns/tpm-update.html
https://nvd.nist.gov/vuln/detail/CVE-2019-16863
https://www.bleepingcomputer.com/news/security/tpm-fail-security-flaws-impact-modern-devices-with-intel-cpus/
https://securityboulevard.com/2019/11/tpm-fail-intel-and-stmicro-fix-26-year-old-vulnerability/
https://thehackernews.com/2019/11/tpm-encryption-keys-hacking.html