BEZPEČNOSTNÝ BULLETIN

Týždeň 22. 04. 2020 - 28. 04. 2020

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:
01439/2020/SK-CERT-102

BEZPEČNOSTNÝ BULLETIN

Týždeň 22. 04. 2020 - 28. 04. 2020

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

21.04.2020

CVE

CVE-2020-6458, CVE-2020-6459, CVE-2020-6460

Zasiahnuté systémy

Google Chrome verzie staršie ako 81.0.4044.122

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/2020/04/stable-channel-update-for-desktop_21.html
https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-google-chrome-could-allow-for-arbitrary-code-execution_2020-054/
https://exchange.xforce.ibmcloud.com/vulnerabilities/180179
https://exchange.xforce.ibmcloud.com/vulnerabilities/180180
https://exchange.xforce.ibmcloud.com/vulnerabilities/180178

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

Identifikátor

Zraniteľnosti Microsoft a Autodesk produktov

Popis

Spoločnosti Microsoft a Autodesk vydali bezpečnostné aktualizácie na svoje produkty, ktoré opravujú viacero bezpečnostných zraniteľností.
Bezpečnostné zraniteľnosti v knižnici Autodesk FBX-SDK 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

15.04.2020

CVE

CVE-2020-7080, CVE-2020-7081, CVE-2020-7082, CVE-2020-7083, CVE-2020-7084, CVE-2020-7085

Zasiahnuté systémy

Autodesk FBX-SDK 2019.5 a staršie
Maya 2019 a staršie
Motion Builder 2019 a staršie
Mudbox 2019 a staršie3ds Max 2020 a staršie
Fusion ATF 8 a staršie
Revit 2020 a staršie
Flame 2019 a staršie
Infraworks 2020 a staršie
Navisworks 2019 Update 4 a staršie
Autodesk AutoCAD 2019 a staršie
Microsoft Office 2016 Click-to-Run (C2R) for 32-bit editions
Microsoft Office 2016 Click-to-Run (C2R) for 64-bit editions
Microsoft Office 2019 for 32-bit editions
Office 365 ProPlus for 32-bit Systems
Office 365 ProPlus for 64-bit Systems
Paint 3D

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://portal.msrc.microsoft.com/en-us/security-guidance/advisory/ADV200004 https://www.autodesk.com/trust/security-advisories/adsk-sa-2020-0002 https://www.cisecurity.org/advisory/draft-ms-isac-cybersecurity-advisory-multiple-vulnerabilities-in-autodesk-fbx-sdk-library-could-allow-for-arbitrary-code-execution-patch-now-tlp-white_2020-053/ https://threatpost.com/microsoft-issues-out-of-band-security-update-for-office-paint-3d/155016/ https://www.securityweek.com/microsoft-out-band-advisory-addresses-autodesk-fbx-vulnerabilities

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

Identifikátor

Juniper JunOS zraniteľnosť

Popis

Spoločnosť Juniper vydala bezpečnostné aktualizácie na svoj produkt JunOS, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť v HTTP/HTTPS komponente umožňuje vzdialenému, neautentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému. Zraniteľnosť je v súčasnosti aktívne zneužívaná útočníkmi.

Dátum prvého zverejnenia varovania

27.04.2020

CVE

CVE-2020-1631

Zasiahnuté systémy

Junos OS verzie staršie ako 12.3X48-D101, 12.3X48-D105, 15.1X49-D211, 15.1X49-D220, 17.4R3-S2, 18.1R3-S10, 18.2R3-S4, 18.3R2-S4, 18.3R3-S2, 18.4R3-S2, 19.1R1-S5, 19.1R3-S1, 19.2R2, 19.3R2-S3, 19.3R3, 19.4R1-S2, 19.4R2, 20.1R1-S1, 20.1R2

Následky

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

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých systémov a vypnúť HTTP/HTTPS služby a funkciu DVPN príkazmi:
user@device# deactivate system services web-management
user@device# deactivate security dynamic-vpn
user@device# commit
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://kb.juniper.net/InfoCenter/index?page=content&id=JSA11021&cat=SIRT_1&actp=LIST

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 8.2
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 je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi vykonávať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

14.04.2020

CVE

CVE-2020-7487, CVE-2020-7488, CVE-2020-7489, CVE-2020-7490

Zasiahnuté systémy

SoMachine
SoMachine Basic
SoMachine Motion
EcoStruxure Machine Expert verzie staršie ako 1.2
EcoStruxure Machine Expert – Basic verzie staršie ako V1.0 SP2
Modicon M100 Logic Controller
Modicon M200 Logic Controller
Modicon M221 Logic Controller
Modicon M218 Logic Controller
Modicon M241 Logic Controller
Modicon M251 Logic Controller
Modicon M258 Logic Controller
Vijeo Designer Basic verzie staršie ako V1.1 HotFix 16
Vijeo Designer

Následky

Neoprávnený prístup do systému
Neoprávnená zmena v systéme
Zneprístupnenie služby
Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých systémov, aplikovať firewallové pravidlá a blokovať port 502/TCP.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.
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://download.schneider-electric.com/files?p_enDocType=Technical+leaflet&p_File_Name=SEVD-2020-105-01_Modicon+M100_M200_M221_and_EcoStruxure%E2%84%A2_Machine+Expert_Basic_Security_Notification.pdf https://download.schneider-electric.com/files?p_enDocType=Technical+leaflet&p_File_Name=SEVD-2020-105-03_Vijeo_Designer_and_Vijeo_Designer_Basic_Security_Notification.pdf https://download.schneider-electric.com/files?p_enDocType=Technical+leaflet&p_File_Name=SEVD-2020-105-02_Modicon+M218_M241_M251_M258_M258_Logic_Controllers_SoMachine_SoMachine_Motion_EcoStruxure_Machine_Expert_Security_Notification.pdf

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

Identifikátor

OpenSSL zraniteľnosť

Popis

Vývojári OpenSSL vydali aktualizáciu na svoj produkt, ktorá opravuje bezpečnostnú zraniteľnosť. Bezpečnostná zraniteľnosť pri nadväzovaní TLS 1.3 spojenia umožňujú vzdialenému, neautentifikovanému útočníkovi spôsobiť zneprístupnenie služieb.

Dátum prvého zverejnenia varovania

21.04.2020

CVE

CVE-2020-1967

Zasiahnuté systémy

OpenSSL verzie staršie ako 1.1.1g

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/180181
https://www.openssl.org/news/secadv/20200421.txt
https://www.securityweek.com/high-severity-vulnerability-openssl-allows-dos-attacks

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

Identifikátor

Apple iOS zraniteľnosť

Popis

Bezpečnostní výskumníci informovali o zraniteľnosti v produkte Apple iOS a iPadOS.
Bezpečnostná zraniteľnosť umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania správ obsahujúcich špeciálne znaky spôsobiť zneprístupnenie služieb.
Zraniteľnosť je v súčasnosti aktívne zneužívaná útočníkmi.

Dátum prvého zverejnenia varovania

23.04.2020

CVE

-

Zasiahnuté systémy

Apple iOS a iPadOS 13

Následky

Zneprístupnenie služby

Odporúčania

Bezpečnostná aktualizácia riešiaca uvedenú zraniteľnosť bola vydaná pre iOS a iPadOS 13.4.5 second beta.Administrátorom a používateľom odporúčame vypnúť notifikačné správy aplikácií a ich náhľady. Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov, nenavštevovali nedôveryhodné webové stránky a neinštalovali neoverené aplikácie.

Zdroje

https://www.hackread.com/ios-text-bomb-bug-crashing-phones-sindhi-characters/
https://www.reddit.com/r/jailbreak/comments/g6rpb8/release_capturetheflag_stop_italian_flag_emoji/
https://appleinsider.com/articles/20/04/23/ios-13-notification-text-bomb-crashes-iphone-ipad

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.4**
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

PrestaShop viacero zraniteľností

Popis

Vývojári e-commerce systému PrestaShop vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje viacero bezpečnostných zraniteľností.
Bezpečnostné zraniteľnosti sú spôsobené nedostatočným overovaním používateľských vstupov a umožňujú vzdialenému, neautentifikovanému útočníkovi získať prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

20.04.2020

CVE

CVE-2020-5264, CVE-2020-5265, CVE-2020-5269, CVE-2020-5270, CVE-2020-5271, CVE-2020-5272, CVE-2020-5276, CVE-2020-5278, CVE-2020-5279, CVE-2020-5285, CVE-2020-5286, CVE-2020-5287, CVE-2020-5288, CVE-2020-5293

Zasiahnuté systémy

PrestaShop verzie staršie ako 1.7.6.5

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnený prístup do systému
Neoprávnená zmena v systéme

Odporúčania

Odporúčame uistiť sa, či Vaše webové stránky nie sú založené na redakčnom systéme PrestaShop so zraniteľnou verziou pluginu. V prípade že áno, zabezpečte aktualizáciu redakčného systému a pluginu.
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://github.com/PrestaShop/PrestaShop/security/advisories/GHSA-48vj-vvr6-jj4f
https://github.com/PrestaShop/PrestaShop/security/advisories/GHSA-7fmr-5vcc-329j
https://github.com/PrestaShop/PrestaShop/security/advisories/GHSA-87jh-7xpg-6v93
https://github.com/PrestaShop/PrestaShop/security/advisories/GHSA-375w-q56h-h7qc
https://github.com/PrestaShop/PrestaShop/security/advisories/GHSA-m2x6-c2c6-pjrx
https://github.com/PrestaShop/PrestaShop/security/advisories/GHSA-rpg3-f23r-jmqv
https://github.com/PrestaShop/PrestaShop/security/advisories/GHSA-74vp-ww64-w2gm
https://github.com/PrestaShop/PrestaShop/security/advisories/GHSA-q6pr-42v5-v97q
https://github.com/PrestaShop/PrestaShop/security/advisories/GHSA-j3r6-33hf-m8wh
https://github.com/PrestaShop/PrestaShop/security/advisories/GHSA-mrpj-67mq-3fr5
https://github.com/PrestaShop/PrestaShop/security/advisories/GHSA-98j8-hvjv-x47j
https://github.com/PrestaShop/PrestaShop/security/advisories/GHSA-cvjj-grfv-f56w
https://github.com/PrestaShop/PrestaShop/security/advisories/GHSA-4wxg-33h3-3w5r
https://github.com/PrestaShop/PrestaShop/security/advisories/GHSA-r6rp-6gv6-r9hq
https://exchange.xforce.ibmcloud.com/vulnerabilities/180127