BEZPEČNOSTNÝ BULLETIN

Týždeň 29. 07. 2020 - 04. 08. 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-192

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

Identifikátor

Mozilla Firefox a Thunderbird - viacero zraniteľností

Popis

Spoločnosť Mozilla vydala bezpečnostné aktualizácie na svoje produkty Firefox, Firefox ESR a Thunderbird, ktoré opravujú 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

28.07.2020

CVE

CVE-2020-15652, CVE-2020-15653, CVE-2020-15654, CVE-2020-15655, CVE-2020-15656, CVE-2020-15657, CVE-2020-15658, CVE-2020-15659, CVE-2020-6463, CVE-2020-6514

Zasiahnuté systémy

Firefox verzie staršie ako 79
Firefox ESR verzie staršie ako 78.1
Thunderbird verzie staršie ako 78.1

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://www.mozilla.org/en-US/security/advisories/mfsa2020-33/
https://www.mozilla.org/en-US/security/advisories/mfsa2020-32/
https://www.mozilla.org/en-US/security/advisories/mfsa2020-30/
https://nakedsecurity.sophos.com/2020/07/28/firefox-79-is-out-its-a-double-update-month-so-patch-now/
https://exchange.xforce.ibmcloud.com/vulnerabilities/185985
https://exchange.xforce.ibmcloud.com/vulnerabilities/185983
https://exchange.xforce.ibmcloud.com/vulnerabilities/185979

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

Identifikátor

Adobe Magento - viacero zraniteľností

Popis

Vývojári E-commerce platformy Magento vydali bezpečnostnú aktualizáciu, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšie bezpečnostné zraniteľnosti 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

28.07.2020

CVE

CVE-2020-9689, CVE-2020-9690, CVE-2020-9691, CVE-2020-9692

Zasiahnuté systémy

Magento Commerce 2 verzie staršie ako 2.4.0 a 2.3.5-p2
Magento Open Source 2 verzie staršie ako 2.4.0 a 2.3.5-p2

Následky

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

Odporúčania

Odporúčame uistiť sa, či Vaše webové stránky nie sú založené na redakčnom systéme Magento v zraniteľnej verzii. V prípade že áno, zabezpečte aktualizáciu redakčného systému a pluginov.
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/magento/apsb20-47.html
https://www.bleepingcomputer.com/news/security/magento-gets-security-updates-for-severe-code-execution-bugs/
https://exchange.xforce.ibmcloud.com/vulnerabilities/185971
https://exchange.xforce.ibmcloud.com/vulnerabilities/185970
https://exchange.xforce.ibmcloud.com/vulnerabilities/185969
https://exchange.xforce.ibmcloud.com/vulnerabilities/185968

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

Identifikátor

Apple iTunes - viacero zraniteľností

Popis

Spoločnosť Apple vydala bezpečnostnú aktualizáciu na svoj produkt iTunes, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšie bezpečnostné zraniteľnosti 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

30.07.2020

CVE

CVE-2020-9862, CVE-2020-9871, CVE-2020-9872, CVE-2020-9873, CVE-2020-9874, CVE-2020-9875, CVE-2020-9876, CVE-2020-9877, CVE-2020-9879, CVE-2020-9893, CVE-2020-9894, CVE-2020-9895, CVE-2020-9910, CVE-2020-9915, CVE-2020-9916, CVE-2020-9919, CVE-2020-9925, CVE-2020-9936, CVE-2020-9937, CVE-2020-9938

Zasiahnuté systémy

iTunes for Windows verzie staršie ako 12.10.5

Následky

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

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých systémov. Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov, nenavštevovali nedôveryhodné webové stránky a neinštalovali neoverené aplikácie.
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://support.apple.com/en-us/HT211293

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

Identifikátor

IBM produkty - viacero zraniteľností

Popis

Spoločnosť IBM vydala bezpečnostné aktualizácie na svoje produkty i2 Analyst's Notebook a Cognos Analytics, ktoré opravujú viacero bezpečnostných zraniteľností.
Bezpečnostné zraniteľnosti sú spôsobené nedostatočným overovaním používateľských vstupov a umožňujú lokálnemu, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

31.07.2020

CVE

CVE-2010-5312, CVE-2016-7103, CVE-2019-0205, CVE-2019-0210, CVE-2019-4366, CVE-2019-4589, CVE-2020-4377, CVE-2020-4549, CVE-2020-4550, CVE-2020-4551, CVE-2020-4552, CVE-2020-4553, CVE-2020-4554

Zasiahnuté systémy

IBM i2 Analyst's Notebook verzia 9.2.1
IBM i2 Analyst's Notebook Premium verzia 9.2.1
IBM Cognos Analytics verzie staršie ako 11.1.7.0
IBM Cognos Analytics verzie staršie ako 11.0.13 FP3

Následky

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

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.ibm.com/support/pages/node/6254694
https://www.ibm.com/support/pages/node/6252853

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

Identifikátor

GRand Unified Bootloader 2 (GRUB2) - bezpečnostné zraniteľnosti

Popis

Bezpečnostní výskumníci informovali o bezpečnostných zraniteľnostiach v GRand Unified Bootloader 2 (GRUB2).
Najzávažnejšia bezpečnostná zraniteľnosť pomenovaná "BootHole" spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi spôsobiť pretečenie zásobníka a následne vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

29.07.2020

CVE

CVE-2020-10713, CVE-2020-14308, CVE-2020-14309, CVE-2020-14310, CVE-2020-14311, CVE-2020-15705, CVE-2020-15706, CVE-2020-15707

Zasiahnuté systémy

GRUB 2 verzie staršie ako 2.06
Operačné systémy založené na UNIX/LINUX (Ubuntu, Debian, SuSE, Red Hat Enterprise Linux)
Operačné systémy Windows

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://eclypsium.com/2020/07/29/theres-a-hole-in-the-boot/ https://www.theregister.com/2020/07/29/grub2_code_exec_flaw/ https://www.forbes.com/sites/daveywinder/2020/07/29/boothole-secure-boot-threat-confirmed-in-most-every-linux-distro-windows-8-and-10-microsoft-ubuntu-redhat-suse-debian-citrix-oracle-vmware/#37721d23666e https://threatpost.com/billions-of-devices-impacted-secure-boot-bypass/157843/ https://ubuntu.com/blog/mitigating-boothole-theres-a-hole-in-the-boot-cve-2020-10713-and-related-vulnerabilities https://access.redhat.com/security/cve/CVE-2020-10713 https://thehackernews.com/2020/07/grub2-bootloader-vulnerability.html https://access.redhat.com/security/vulnerabilities/grub2bootloader https://www.debian.org/security/2020-GRUB-UEFI-SecureBoot/ https://wiki.ubuntu.com/SecurityTeam/KnowledgeBase/GRUB2SecureBootBypass https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV200011 https://support.hp.com/us-en/document/c06707446 https://techhub.hpe.com/eginfolib/securityalerts/Boot_Hole/boot_hole.html https://kb.vmware.com/s/article/80181

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

Identifikátor

Dell EMC iDRAC9 - zraniteľnosť

Popis

Spoločnosť Dell vydala bezpečnostnú aktualizáciu na svoj produkt EMC iDRAC9, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť umožňuje vzdialenému, autentifikovanému útočníkovi získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

07.07.2020

CVE

CVE-2020-5366

Zasiahnuté systémy

Dell EMC iDRAC9 verzie staršie ako 4.20.20.20

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
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.dell.com/support/article/sk-sk/sln322125/dsa-2020-128-idrac-local-file-inclusion-vulnerability?lang=en
https://threatpost.com/researchers-warn-of-high-severity-dell-poweredge-server-flaw/157795/