BEZPEČNOSTNÝ BULLETIN

Týždeň 16. 03. 2022 - 22. 03. 2022

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Google Chrome - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
02.	ClickHouse produkt - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
03.	ABB OPC Server pre AC 800M - bezpečnostná zraniteľnosť	Vysoká	**8.4**
04.	Dell BIOS - viacero bezpečnostných zraniteľností	Vysoká	**8.2**
05.	IBM Spectrum Protect Server - bezpečnostná zraniteľnosť	Vysoká	**7.5**
06.	OpenSSL knižnica - bezpečnostná zraniteľnosť	Vysoká	**7.5**

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:
01794/2022/SK-CERT-709

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

Identifikátor

Google Chrome - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Google vydala bezpečnostnú aktualizáciu na produkt Chrome, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom povrhnutia špeciálne vytvorenej webovej stránky, vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

15.03.2022

CVE

CVE-2022-0971, CVE-2022-0972, CVE-2022-0973, CVE-2022-0974, CVE-2022-0975, CVE-2022-0976, CVE-2022-0977, CVE-2022-0978, CVE-2022-0979, CVE-2022-0980

Zasiahnuté systémy

Google Chrome vo verzii staršej ako 99.0.4844.74

Následky

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

Odporúčania

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

Zdroje

https://chromereleases.googleblog.com/2022/03/stable-channel-update-for-desktop_15.html
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0979
https://exchange.xforce.ibmcloud.com/vulnerabilities/221869

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

Identifikátor

ClickHouse produkt - viacero bezpečnostných zraniteľností

Popis

Vývojári nástroja ClickHouse vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom povrhnutia špeciálne vytvorených súborov, vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

15.03.2022

CVE

CVE-2021-42387, CVE-2021-42388, CVE-2021-42389, CVE-2021-42390, CVE-2021-42391, CVE-2021-43304, CVE-2021-43305, CVE-2021-44521

Zasiahnuté systémy

ClickHouse vo verzii staršej ako v21.10.2.15-stable

Následky

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

Odporúčania

Administrátorom a používateľom 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.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.
Administrátorom odporúčame limitovať prístup k administratívnemu rozhraniu a jeho funkciám zavedením zoznamu pre riadenie prístupov (ACL).

Zdroje

https://thehackernews.com/2022/03/multiple-flaws-uncovered-in-clickhouse.html
https://jfrog.com/blog/7-rce-and-dos-vulnerabilities-found-in-clickhouse-dbms/
https://github.com/ClickHouse/ClickHouse/releases/tag/v21.10.2.15-stable
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-43305
https://exchange.xforce.ibmcloud.com/vulnerabilities/221841

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.4**
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

ABB OPC Server pre AC 800M - bezpečnostná zraniteľnosť

Popis

Spoločnosť ABB vydala bezpečnostnú aktualizáciu na produkt OPC Server pre AC 800M, ktorá opravuje bezpečnostnú zraniteľnosť. Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje autentifikovanému útočníkovi s právomocami používateľa, ktorý sa nachádza v rovnakom sieťovom segmente eskalovať svoje privilégiá a následne vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

16.03.2022

CVE

CVE-2021-22284

Zasiahnuté systémy

OPC Server pre AC 800M vo verzii staršej ako v6.1.0-0
OPC Server pre AC 800M vo verzii staršej ako 6.0.0-4

Následky

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

Odporúčania

Administrátorom a používateľom 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.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

https://us-cert.cisa.gov/ics/advisories/icsa-22-074-01
https://search.abb.com/library/Download.aspx?DocumentID=7PAA000908&LanguageCode=en&DocumentPartId=&Action=Launch

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

Identifikátor

Dell BIOS - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Dell vydala bezpečnostnú aktualizáciu na svoje portfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami administrátora vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

10.03.2022

CVE

CVE-2022-24415, CVE-2022-24416, CVE-2022-24419, CVE-2022-24420, CVE-2022-24421

Zasiahnuté systémy
Alienware 13 R3 s firmware vo verzii staršej ako 1.16.1
Alienware 15 R3 s firmware vo verzii staršej ako 1.16.1
Alienware 15 R4 s firmware vo verzii staršej ako 1.17.0
Alienware 17 R4 s firmware vo verzii staršej ako 1.16.1
Alienware 17 R5 s firmware vo verzii staršej ako 1.17.0
Alienware Area 51m R1 s firmware vo verzii staršej ako 1.18.0
Alienware Area 51m R2 s firmware vo verzii staršej ako 1.13.0
Alienware Aurora R8 s firmware vo verzii staršej ako 1.0.20
Alienware m15 R2 s firmware vo verzii staršej ako 1.12.0
Alienware m15 R3 s firmware vo verzii staršej ako 1.14.0
Alienware m15 R4 s firmware vo verzii staršej ako 1.8.0
Alienware m17 R2 s firmware vo verzii staršej ako 1.12.0
Alienware m17 R3 s firmware vo verzii staršej ako 1.14.0
Alienware m17 R4 s firmware vo verzii staršej ako 1.8.0
Alienware x15 R1 s firmware vo verzii staršej ako 1.7.0
Alienware x17 R1 s firmware vo verzii staršej ako 1.7.0
Dell Edge Gateway 3000 Series s firmware vo verzii staršej ako 1.7.0
Dell Edge Gateway 5000/5100 s firmware vo verzii staršej ako 1.17.0
Dell Embedded Box PC 3000 s firmware vo verzii staršej ako 1.13.0
Dell Embedded Box PC 5000 s firmware vo verzii staršej ako 1.14.0
Inspiron 14 3473 s firmware vo verzii staršej ako 1.14.0
Inspiron 15 3573 s firmware vo verzii staršej ako 1.14.0
Inspiron 15 5566 s firmware vo verzii staršej ako 1.18.0
Inspiron 3277 s firmware vo verzii staršej ako 1.19.0
Inspiron 3465 s firmware vo verzii staršej ako 1.12.0
Inspiron 3477 s firmware vo verzii staršej ako 1.19.0
Inspiron 3482 s firmware vo verzii staršej ako 1.13.0
Inspiron 3502 s firmware vo verzii staršej ako 1.7.0
Inspiron 3510 s firmware vo verzii staršej ako 1.6.0
Inspiron 3565 s firmware vo verzii staršej ako 1.12.0
Inspiron 3582 s firmware vo verzii staršej ako 1.13.0
Inspiron 3782 s firmware vo verzii staršej ako 1.13.0
Latitude 3379 s firmware vo verzii staršej ako 1.0.34
Vostro 14 5468 s firmware vo verzii staršej ako 1.19.0
Vostro 15 5568 s firmware vo verzii staršej ako 1.19.0
Vostro 3267 s firmware vo verzii staršej ako 1.20.0
Vostro 3268 s firmware vo verzii staršej ako 1.20.0
Vostro 3572 s firmware vo verzii staršej ako 1.14.0
Vostro 3582 s firmware vo verzii staršej ako 1.13.0
Vostro 3660 s firmware vo verzii staršej ako 1.20.0
Vostro 3667 s firmware vo verzii staršej ako 1.20.0
Vostro 3668 s firmware vo verzii staršej ako 1.20.0
Vostro 3669 s firmware vo verzii staršej ako 1.20.0
Wyse 7040 Thin Client s firmware vo verzii staršej ako 1.15.0
XPS 8930 s firmware vo verzii staršej ako 1.1.21

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

Odporúčania
Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov. Po odstránení zraniteľností, ktoré mohli spôsobiť lokálne 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://thehackernews.com/2022/03/new-dell-bios-bugs-affect-millions-of.html https://binarly.io/posts/AMI_UsbRt_Repeatable_Failures_A_6_year_old_attack_vector_still_affecting_millions_of_enterprise_devices/index.html https://www.dell.com/support/kbdoc/sk-sk/000197057/dsa-2022-053

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

Identifikátor

IBM Spectrum Protect Server - bezpečnostná zraniteľnosť

Popis

Spoločnosť IBM vydala bezpečnostnú aktualizáciu na produkt Spectrum Protect Server, ktorá opravuje bezpečnostnú zraniteľnosť. Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

18.03.2022

CVE

CVE-2022-22394

Zasiahnuté systémy

IBM Spectrum Protect Server vo verzii staršej ako 8.1.14.100

Následky

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

Odporúčania

Administrátorom a používateľom 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.ibm.com/support/pages/node/6564745
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22394
https://exchange.xforce.ibmcloud.com/vulnerabilities/222147

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

Identifikátor

OpenSSL knižnica - bezpečnostná zraniteľnosť

Popis

Vývojári knižnice OpenSSL vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvoreného certifikátu, spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

15.03.2022

CVE

CVE-2022-0778

Zasiahnuté systémy

OpenSSL vo verzii staršej ako 1.0.2zd
OpenSSL vo verzii staršej ako 1.1.1n
OpenSSL vo verzii staršej ako 3.0.2

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Odporúčame uistiť sa, či Vaše aplikácie nevyužívajú frameworky, knižnice, pluginy, SDK alebo moduly v zraniteľnej verzii. V prípade, že áno, zabezpečte aktualizáciu všetkých komponentov, od ktorých závisí vaša aplikácia, na aktuálne verzie bez známych bezpečnostných zraniteľností.

Zdroje

https://www.bleepingcomputer.com/news/security/openssl-cert-parsing-bug-causes-infinite-denial-of-service-loop/
https://www.openssl.org/news/secadv/20220315.txt
https://bugzilla.redhat.com/show_bug.cgi?id=2062202
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0778
https://exchange.xforce.ibmcloud.com/vulnerabilities/221911