BEZPEČNOSTNÝ BULLETIN

Týždeň 29. 06. 2022 - 05. 07. 2022

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Mozilla Firefox a Thunderbird - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
02.	Google Chrome - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
03.	Apache HTTP Server - bezpečnostná zraniteľnosť	Vysoká	**8.1**
04.	Autodesk AutoCAD a Navisworks - viacero bezpečnostných zraniteľností	Vysoká	**7.8**
05.	RARLAB RAR/Unix - bezpečnostná zraniteľnosť	Vysoká	**7.5**
06.	Microsoft Service Fabric - bezpečnostná zraniteľnosť	Stredná	**6.7**

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-816

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

Identifikátor

Mozilla Firefox a Thunderbird - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Mozilla Foundation vydala bezpečnostné aktualizácie na produkty Mozilla Firefox, Firefox ESR, Firefox pre iOA a Thunderbird, ktoré opravujú viacero bezpečnostných zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorenej webovej stránky vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

28.06.2022

CVE

CVE-2022-2200, CVE-2022-2226, CVE-2022-31744, CVE-2022-31746, CVE-2022-34468, CVE-2022-34469, CVE-2022-34470, CVE-2022-34471, CVE-2022-34472, CVE-2022-34473, CVE-2022-34474, CVE-2022-34475, CVE-2022-34476, CVE-2022-34477, CVE-2022-34478, CVE-2022-34479, CVE-2022-34480, CVE-2022-34481, CVE-2022-34482, CVE-2022-34483, CVE-2022-34484, CVE-2022-34485

Zasiahnuté systémy

Mozilla Firefox vo verzii staršej ako 102
Firefox ESR vo verzii staršej ako 91.11
Firefox pre iOS vo verzii staršej ako
Thunderbird vo verzii staršej ako 91.11 a 102

Následky

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

Odporúčania

Administrátorom a používateľom 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/mfsa2022-26/
https://www.mozilla.org/en-US/security/advisories/mfsa2022-25/
https://www.mozilla.org/en-US/security/advisories/mfsa2022-24/
https://www.mozilla.org/en-US/security/advisories/mfsa2022-27/

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-816

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 bezpečnostné aktualizácie na internetové prehliadače Chrome, ktorá opravuje viacero kritických bezpečnostných zraniteľností.
Najzávažnejšia kritická bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorenej webstránky vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.
Zraniteľnosť je aktuálne aktívne zneužívaná útočníkmi.

Dátum prvého zverejnenia varovania

04.07.2022

CVE

CVE-2022-2294, CVE-2022-2295, CVE-2022-2296

Zasiahnuté systémy

Google Chrome 103 pre Android vo verzii staršej ako 103.0.5060.71
Google Chrome 103 pre Windows a Mac vo verzii staršej ako 103.0.5060.114

Následky

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

Odporúčania

Administrátorom a používateľom 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://threatpost.com/actively-exploited-chrome-bug/180118/
https://chromereleases.googleblog.com/

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.1**
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Apache HTTP Server - bezpečnostná zraniteľnosť

Popis

Spoločnosť Apache vydala bezpečnostnú aktualizáciu na svoju serverovú platformu Apache HTTP Server, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej požiadavky vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

29.06.2022

CVE

CVE-2022-22721

Zasiahnuté systémy

Apache HTTP Server vo verzii staršej 2.4.53

Následky

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

Odporúčania

Administrátorom a používateľom 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://www.zerodayinitiative.com/advisories/ZDI-22-876/
https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2022-22721

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

Identifikátor

Autodesk AutoCAD a Navisworks - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Autodesk vydala bezpečnostnú aktualizáciu na svoje portfólio produktov Autodesk (AutoCAD a Navisworks), ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

30.06.2022

CVE

CVE-2022-25789, CVE-2022-25790, CVE-2022-25791, CVE-2022-25792, CVE-2022-25796, CVE-2022-27528, CVE-2022-27868

Zasiahnuté systémy

Navisworks vo verzii staršej ako 2022.2, 2020.5, 2019.7
AutoCAD vo verzii staršej ako 2023.0.1, 2022.1.2, 2021.1.2, 2020.1.5, 2019.1.4**
AutoCAD® Architecture vo verzii staršej ako 2023.0.1, 2022.1.2, 2021.1.2, 2020.1.5, 2019.1.4**
AutoCAD® Electrical vo verzii staršej ako 2023.0.1, 2022.1.2, 2021.1.2, 2020.1.5, 2019.1.4**
AutoCAD® Map 3D vo verzii staršej ako 2023.0.1, 2022.1.2, 2021.1.2, 2020.1.5, 2019.1.4**
AutoCAD® Mechanical vo verzii staršej ako 2023.0.1, 2022.1.2, 2021.1.2, 2020.1.5, 2019.1.4**
AutoCAD® MEP vo verzii staršej ako 2023.0.1, 2022.1.2, 2021.1.2, 2020.1.5, 2019.1.4**
AutoCAD® Plant 3D vo verzii staršej ako 2023.0.1, 2022.1.2, 2021.1.2, 2020.1.5, 2019.1.4**
AutoCAD® LT vo verzii staršej ako 2023.0.1, 2022.1.2, 2021.1.2, 2020.1.5, 2019.1.4
AutoCAD® Mac vo verzii staršej ako 2022.2.2
AutoCAD® Mac LT vo verzii staršej ako 2022.2.2
Civil 3D® vo verzii staršej ako 2023.0.1, 2022.1.2, 2021.1.2, 2020.1.5, 2019.1.4**
Advance Steel vo verzii staršej ako 2023.0.1, 2022.1.2, 2021.1.2, 2020.1.5, 2019.1.4**

Následky

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

Odporúčania

Administrátorom a používateľom 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://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0005
https://www.zerodayinitiative.com/advisories/ZDI-22-944/

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

Identifikátor

RARLAB RAR/Unix - bezpečnostná zraniteľnosť

Popis

Spoločnosť win.rar GmbH vydala bezpečnostnú aktualizáciu na svoj produkt RAR/Unix, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvoreného súboru vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

17.05.2022

CVE

CVE-2022-30333

Zasiahnuté systémy

RAR/Unix vo verzii staršej ako 6.12

Následky

Neoprávnená zmena v systéme

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://nvd.nist.gov/vuln/detail/CVE-2022-30333

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 6.7
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Microsoft Service Fabric - bezpečnostná zraniteľnosť

Popis

Spoločnosť Microsoft vydala bezpečnostnú aktualizáciu na cloudovú platformu Microsoft Service Fabric, ktorá opravuje bezpečnostnú zraniteľnosť. MS Service Fabric je používaný v rámci cloudových služieb MS Azure.

Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami administrátora pomocou zneužitia komponentu "Container" eskalovať svoje privilégiá a vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

14.06.2022

CVE

CVE-2022-30137

Zasiahnuté systémy

Microsoft Service Fabric vo verzii staršej ako 9.0 Cumulative Update 1.0 Release

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://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30137
https://unit42.paloaltonetworks.com/fabricscape-cve-2022-30137/