BEZPEČNOSTNÝ BULLETIN

Týždeň 25. 05. 2022 - 31. 05. 2022

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:
01794/2022/SK-CERT-770

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

Identifikátor

iOS a iPadOS - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Apple vydala bezpečnostnú aktualizáciu na knižnicu Webkit vo svojich produktoch iOS a iPadOS, ktorá opravuje viacero bezpečnostných zraniteľností. Knižnica webkit sa používa vo väčšine iOS aplikácií na zobrazovanie multimediálneho obsahu.
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

24.05.2022

CVE

CVE-2021-30809, CVE-2021-30818, CVE-2021-30836, CVE-2021-30846, CVE-2021-30848, CVE-2021-30849, CVE-2021-30851, CVE-2021-30884, CVE-2021-30897, CVE-2021-31005, CVE-2021-31008

Zasiahnuté systémy

iOS a iPadOS Webkit vo verzii staršej ako 15

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame bezodkladne 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://nvd.nist.gov/vuln/detail/CVE-2021-31008
https://support.apple.com/en-us/HT212814

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 svoj webový prehliadač Google Chrome, ktorá opravuje viacero bezpečnostných zraniteľností.
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

24.05.2022

CVE

CVE-2022-1853, CVE-2022-1854, CVE-2022-1855, CVE-2022-1856, CVE-2022-1857, CVE-2022-1858, CVE-2022-1859, CVE-2022-1860, CVE-2022-1861, CVE-2022-1862, CVE-2022-1863, CVE-2022-1864, CVE-2022-1865, CVE-2022-1866, CVE-2022-1867, CVE-2022-1868, CVE-2022-1869, CVE-2022-1870, CVE-2022-1871, CVE-2022-1872, CVE-2022-1873, CVE-2022-1874, CVE-2022-1875, CVE-2022-1876

Zasiahnuté systémy

Google Chrome vo verzii staršej ako 102.0.5005.61

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/2022/05/stable-channel-update-for-desktop_24.html
https://www.redpacketsecurity.com/google-chrome-indexed-db-code-execution-cve-2022-1853/

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

Identifikátor

Fidelis Network a Fidelis Deception - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Fidelis Cybersecurity vydala bezpečnostnú aktualizáciu na svoje produkty Fidelis Network a Fidelis Deception, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej HTTP požiadavky vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

17.05.2022

CVE

CVE-2022-24388, CVE-2022-24389, CVE-2022-24391, CVE-2022-24392, CVE-2022-24393, CVE-2022-24394

Zasiahnuté systémy

Fidelis Network vo verzii staršej ako 9.4.5
Fidelis Deception vo verzii staršej ako 9.4.5

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://nvd.nist.gov/vuln/detail/CVE-2022-24394
https://www.cve.org/CVERecord?id=CVE-2022-24394
https://support.fidelissecurity.com/hc/en-us/article_attachments/6212028955411/Security_Advisory_20220515.pdf

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.3**
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

KiviCare WordPress plugin - bezpečnostná zraniteľnosť

Popis

Vývojári pluginu KiviCare vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom SQL injekcie vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

23.05.2022

CVE

CVE-2022-0786

Zasiahnuté systémy

KiviCare plugin vo verzii staršej ako 2.3.9

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://patchstack.com/database/vulnerability/kivicare-clinic-management-system/wordpress-kivicare-plugin-2-3-8-unauthenticated-sql-injection-sqli-vulnerability

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.0**
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Guzzle - bezpečnostná zraniteľnosť

Popis

Vývojári PHP HTTP klienta Guzzle vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej HTTP odpovede z webového servera získať neoprávnený prístup k citlivým údajom a vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

25.05.2022

CVE

CVE-2022-29248

Zasiahnuté systémy

Guzzle vo verzii staršej ako 7.5.0

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť získanie prístupu k citlivým údajom 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://nvd.nist.gov/vuln/detail/CVE-2022-29248
https://github.com/guzzle/guzzle/security/advisories/GHSA-cwmx-hcrq-mhc3

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

Identifikátor

Adobe produkty - viacero bezpečnostných zraniteľností

Popis

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

Dátum prvého zverejnenia varovania

25.05.2022

CVE

CVE-2021-44701, CVE-2021-44702, CVE-2021-44703, CVE-2021-44704, CVE-2021-44705, CVE-2021-44706, CVE-2021-44707, CVE-2021-44708, CVE-2021-44709, CVE-2021-44710, CVE-2021-44711, CVE-2021-44712, CVE-2021-44713, CVE-2021-44714, CVE-2021-44715, CVE-2021-44739, CVE-2021-44740, CVE-2021-44741, CVE-2021-44742, CVE-2021-45060, CVE-2021-45061, CVE-2021-45062, CVE-2021-45063, CVE-2021-45064, CVE-2021-45067, CVE-2021-45068, CVE-2022-24091, CVE-2022-24092

Zasiahnuté systémy

Acrobat DC vo verzii staršej ako 21.011.20039
Acrobat Reader DC vo verzii staršej ako 21.011.20039
Acrobat 2020 vo verzii staršej ako 20.004.30020
Acrobat Reader 2020 vo verzii staršej ako 20.004.30020
Acrobat 2017 vo verzii staršej ako 17.011.30207
Acrobat Reader 2017 vo verzii staršej ako 17.011.30207

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://nvd.nist.gov/vuln/detail/CVE-2021-44705
https://helpx.adobe.com/security/products/acrobat/apsb22-01.html

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

Identifikátor

Citrix ADC a Citrix Gateway - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť Citrix Systems vydala bezpečnostné aktualizácie na produkty Citrix ADC a Citrix Gateway, ktoré opravujú dve bezpečnostné zraniteľnosti.
Bezpečnostné zraniteľnosti by vzdialený útočník mohol zneužiť na zneprístupnenie služby.
Bezpečnostnú zraniteľnosť s označením CVE-2022-27507 je možné zneužiť výlučne na zariadeniach Citrix ADC a Citrix Gateway s aktivovaným DTLS a konfiguráciou HDX Insight pre EDT traffic alebo SmartControl.

Dátum prvého zverejnenia varovania

25.05.2022

CVE

CVE-2022-27507, CVE-2022-27508

Zasiahnuté systémy

Citrix ADC a Citrix Gateway vo verzii staršej ako 13.1-21.50
Citrix ADC a Citrix Gateway vo verzii staršej ako 13.0-85.19
Citrix ADC a Citrix Gateway vo verzii staršej ako 12.1-64.17
Citrix ADC 12.1-FIPS vo verzii staršej ako 12.1-55.278
Citrix ADC 12.1-NDcPP vo verzii staršej ako 12.1-55.278

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://support.citrix.com/article/CTX457048