BEZPEČNOSTNÝ BULLETIN

Týždeň 01. 06. 2022 - 07. 06. 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-775

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

Identifikátor

Horde Webmail - bezpečnostná zraniteľnosť

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnosti webového mailového klienta Horde.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvoreného e-mailu vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému. Na spustenie škodlivého kódu stačí používateľovi otvoriť správu.
Zraniteľnosť je v súčasnosti aktívne zneužívaná útočníkmi.

Dátum prvého zverejnenia varovania

31.05.2022

CVE

CVE-2022-30287

Zasiahnuté systémy

Horde Groupware Webmail Edition vo všetkých verziách

Následky

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

Odporúčania

Odporúčame zvážiť použitie iných webových mailových klientov s aktívnou podporou.
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://blog.sonarsource.com/horde-webmail-rce-via-email/
https://securityaffairs.co/wordpress/131870/hacking/rce-flaw-horde-webmail.html

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

Identifikátor

TikTok pre Android - bezpečnostná zraniteľnosť

Popis

Spoločnosť ByteDance vydala bezpečnostnú aktualizáciu pre TikTok pre platformu Android, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorenej URL získať úplnú kontrolu nad používateľským kontom obete.

Dátum prvého zverejnenia varovania

01.06.2022

CVE

CVE-2022-28799

Zasiahnuté systémy

TikTok pre platformu Android vo verzii staršej ako 23.8.4

Následky

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 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://www.redpacketsecurity.com/tiktok-account-hijacking-cve-2022-28799/
https://github.com/Ch0pin/security-advisories/security/advisories/GHSA-v39p-88q5-5cvr

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

Identifikátor

Mozilla Firefox, Firefox ESR a Thunderbird - viacero kritických bezpečnostných zraniteľností

Popis

Spoločnosť Mozilla vydala bezpečnostnú aktualizáciu na svoje portfólio produktov, 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 webovej stránky, vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

31.05.2022

CVE

CVE-2022-1834, CVE-2022-1887, CVE-2022-1919, CVE-2022-31736, CVE-2022-31737, CVE-2022-31738, CVE-2022-31739, CVE-2022-31740, CVE-2022-31741, CVE-2022-31742, CVE-2022-31743, CVE-2022-31744, CVE-2022-31745, CVE-2022-31747, CVE-2022-31748

Zasiahnuté systémy

Firefox vo verzii staršej ako 101
Firefox pre iOS vo verzii staršej ako 101
Thunderbird vo verzii staršej ako 91.10
Firefox ESR vo verzii staršej ako 91.10

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://www.mozilla.org/en-US/security/advisories/mfsa2022-23/
https://www.mozilla.org/en-US/security/advisories/mfsa2022-22/
https://www.mozilla.org/en-US/security/advisories/mfsa2022-21/
https://www.mozilla.org/en-US/security/advisories/mfsa2022-20/

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

Identifikátor

WordPress plugin HTML2WP - viacero bezpečnostných zraniteľností

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnostiach WordPress pluginu HTML2WP. Najzávažnejšia 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

06.06.2022

CVE

CVE-2022-1572, CVE-2022-1573, CVE-2022-1574

Zasiahnuté systémy

HTML2WP WordPress plugin - všetky verzie

Následky

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

Odporúčania

Na uvedené zraniteľnosti v súčasnosti nie sú dostupné aktualizácie a plugin bol v rámci CMS Wordpress odstránený zo zoznamu pluginov na stiahnutie. Administrátorom odporúčame uistiť sa, či ich webové stránky a aplikácie nevyužívajú predmetný plugin a do vydania bezpečnostných záplat plugin deaktivovať a odinštalovať.
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/html2wp/wordpress-html2wp-plugin-1-0-0-unauthenticated-arbitrary-file-upload-vulnerability
https://wordpress.org/plugins/html2wp/

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

Identifikátor

FreeBSD - bezpečnostná zraniteľnosť

Popis

Vývojári operačného systému FreeBSD vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nesprávnom spracovaní 802.11.Wi-Fi beacon rámcov a umožňuje neautentifikovanému útočníkovi, ktorý sa nachádza v rovnakom sieťovom segmente, prostredníctvom prepísania kernel pamäte vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

06.04.2022

CVE

CVE-2022-23088

Zasiahnuté systémy

FreeBSD vo verzii staršej ako 13.1-STABLE
FreeBSD vo verzii staršej ako 13.1-RC1-p1
FreeBSD vo verzii staršej ako 13.0-RELEASE-p11
FreeBSD vo verzii staršej ako 12.3-STABLE
FreeBSD vo verzii staršej ako 12.3-RELEASE-p5

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.zerodayinitiative.com/advisories/ZDI-22-806/
https://www.freebsd.org/security/advisories/FreeBSD-SA-22:07.wifi_meshid.asc

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

Identifikátor

Apache Traffic Server - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť Apache vydala bezpečnostnú aktualizáciu na proxy server Apache, ktorá opravuje dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii mechanizmov autentifikácie a umožňuje vzdialenému, neautentifikovanému útočníkovi zrealizovať MITM (Man In The Middle) útok s následkom úplného narušenia dôvernosti, integrity a dostupnosti komunikácie.

Dátum prvého zverejnenia varovania

23.05.2022

CVE

CVE-2021-44040, CVE-2021-44759

Zasiahnuté systémy

ATS vo verziách 8.0.0 až 8.1.3
ATS vo verziách 9.0.0 až 9.1.1

Následky

Úplné narušenie dôvernosti, integrity a dostupnosti systému

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://lists.apache.org/thread/zblwzcfs9ryhwjr89wz4osw55pxm6dx6
https://nvd.nist.gov/vuln/detail/CVE-2021-44759#range-7766051

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

Identifikátor

Zyxel - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Zyxel Networks vydala bezpečnostnú aktualizáciu na svoje portfólio produktov, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi prostredníctvom zaslania špeciálne upravených príkazov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

27.05.2022

CVE

CVE-2022-0734, CVE-2022-0910, CVE-2022-26531, CVE-2022-26532

Zasiahnuté systémy

Kompletný zoznam zasiahnutých zariadení možno nájsť na https://www.zyxel.com/support/multiple-vulnerabilities-of-firewalls-AP-controllers-and-APs.shtml

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.zyxel.com/support/multiple-vulnerabilities-of-firewalls-AP-controllers-and-APs.shtml
https://nvd.nist.gov/vuln/detail/CVE-2022-26532