BEZPEČNOSTNÝ BULLETIN

Týždeň 23. 09. 2022 - 29. 09. 2022

OBSAH BEZPEČNOSTNÉHO BULLETINU

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

Identifikátor

Mozilla produkty - viacero bezpečnostných zraniteľností

Popis

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

20.09.2022

CVE

CVE-2022-3033, CVE-2022-3155, CVE-2022-3266, CVE-2022-40956, CVE-2022-40957, CVE-2022-40958, CVE-2022-40959, CVE-2022-40960, CVE-2022-40961, CVE-2022-40962

Zasiahnuté systémy

Mozilla Firefox vo verzii staršej ako 105
Firefox ESR vo verzii staršej ako 102.3
Thunderbird vo verzii staršej ako 102.3

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/mfsa2022-39/
https://www.mozilla.org/en-US/security/advisories/mfsa2022-42/
https://www.mozilla.org/en-US/security/advisories/mfsa2022-41/
https://www.mozilla.org/en-US/security/advisories/mfsa2022-40/

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

Identifikátor

InsydeH2O SMM driver - viacero bezpečnostných zraniteľností

Popis

Spoločnosť InsydeH2O vydala bezpečnostnú aktualizáciu na SMM ovládača produktu InsydeH2O, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami administrátora vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

21.09.2022

CVE

CVE-2022-35408, CVE-2022-35893, CVE-2022-35894, CVE-2022-35895, CVE-2022-35896, CVE-2022-36338, CVE-2022-36448

Zasiahnuté systémy

InsydeH2O UEFI Kernel 5.0 (IB02961492 vo verzii staršej ako 05.09.37)
InsydeH2O UEFI Kernel 5.1 (IB02961492 vo verzii staršej ako 05.17.37)
InsydeH2O UEFI Kernel 5.2 (IB02961492 vo verzii staršej ako 05.27.29)
InsydeH2O UEFI Kernel 5.3 (IB02961492 vo verzii staršej ako 05.36.29)
InsydeH2O UEFI Kernel 5.4 (IB02961492 vo verzii staršej ako 05.44.29)
InsydeH2O UEFI Kernel 5.5 (IB02961492 vo verzii staršej ako 05.52.29)

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://binarly.io/advisories/BRLY-2022-026/index.html
https://binarly.io/advisories/BRLY-2022-025/index.html
https://binarly.io/advisories/BRLY-2022-024/index.html
https://binarly.io/advisories/BRLY-2022-023/index.html
https://binarly.io/advisories/BRLY-2022-022/index.html
https://binarly.io/advisories/BRLY-2022-018/index.html
https://binarly.io/advisories/BRLY-2022-017/index.html
https://www.insyde.com/security-pledge#InsydeSept212022

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.7
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Harbor - viacero bezpečnostných zraniteľností

Popis

Vývojári open-source nástroja Harbor 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 zaslania špeciálne vytvorenej požiadavky vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

30.08.2022

CVE

CVE-2022-31666, CVE-2022-31667, CVE-2022-31669, CVE-2022-31670, CVE-2022-31671

Zasiahnuté systémy

Harbor vo verzii staršej ako v2.5.2

Následky

Neoprávnená zmena v systéme

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://github.com/goharbor/harbor/security/advisories/GHSA-3637-v6vq-xqqw
https://www.oxeye.io/press-releases/high-severity-idor-vulnerabilities-identified-by-oxeye-research-team-in-cncf-harbor-project-by-vmware

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

Identifikátor

BIND 9 - viacero bezpečnostných zraniteľností

Popis

Vývojári DNS systému BIND 9 vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne vytvorených požiadaviek spôsobiť zahltenie pamäte a následné zneprístupnenie služby.

Dátum prvého zverejnenia varovania

23.09.2022

CVE

CVE-2022-2906, CVE-2022-3080, CVE-2022-38177, CVE-2022-38178

Zasiahnuté systémy

BIND (stable branch) vo verzii staršej ako 9.18
BIND (development version) vo verzii staršej ako 9.19
BIND (Extended Support Version) vo verzii staršej ako 9.16

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.securityweek.com/bind-updates-patch-high-severity-vulnerabilities
https://nvd.nist.gov/vuln/detail/CVE-2022-2906

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.4
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

BOSCH BVMS a VIDEOJET Decoder - bezpečnostná zraniteľnosť

Popis

Spoločnosť BOSCH vydala bezpečnostné aktualizácie na produkty BVMS a VIDEOJET Decoder, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi zrealizovať MITM (Man In The Middle) útok a získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

21.09.2022

CVE

CVE-2022-32540

Zasiahnuté systémy

Bosch BVMS vo verzii staršej ako 11.1.1
Bosch BVMS Viewer vo verzii staršej ako 11.1.1
Bosch VIDEOJET Decoder VJD-7513 vo verzii staršej ako 10.31.0005

Následky

Neoprávnený prístup k citlivým údajom

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://psirt.bosch.com/security-advisories/bosch-sa-464066-bt.html

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 6.1
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

netlify-ipx - bezpečnostná zraniteľnosť

Popis

Vývojári nástroja na optimalizáciu obrázkov pre Netlify (Next.js repozitár netlify-ipx) 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 požiadavky získať neoprávnený prístup k citlivým údajom a vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

23.09.2022

CVE

CVE-2022-39239

Zasiahnuté systémy

netlify-ipx vo verzii staršej ako 1.2.3

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme

Odporúčania

Odporúčame uistiť sa, či vo svojich aplikáciách nevyužívate netlify-ipx v zraniteľných verziách. V prípade, že áno, administrátorom 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-2022-39239
https://samcurry.net/universal-xss-on-netlifys-next-js-library/

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-890