BEZPEČNOSTNÝ BULLETIN

Týždeň 18. 05. 2022 - 24. 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-765

BEZPEČNOSTNÝ BULLETIN

Týždeň 18. 05. 2022 - 24. 05. 2022

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

Identifikátor

Mozilla produkty - dve bezpečnostné zraniteľnosti

Popis

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

20.05.2022

CVE

CVE-2022-1529, CVE-2022-1802

Zasiahnuté systémy

Mozilla Firefox vo verzii staršej ako 100.0.2
Firefox ESR vo verzii staršej ako 91.9.1
Firefox pre Android vo verzii staršej ako 100.3
Thunderbird vo verzii staršej ako 91.9.1

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://exchange.xforce.ibmcloud.com/vulnerabilities/227037
https://exchange.xforce.ibmcloud.com/vulnerabilities/227036
https://www.mozilla.org/en-US/security/advisories/mfsa2022-19/#CVE-2022-1802

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 8.6
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Mitsubishi Electric MELSEC iQ-F produkty - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť Mitsubishi Electric vydala bezpečnostnú aktualizáciu na produkt MELSEC iQ-F Series Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne vytvorených paketov, spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

19.05.2022

CVE

CVE-2022-25161, CVE-2022-25162

Zasiahnuté systémy

MELSEC iQ-F FX5U-xMy/z x=32,64,80, y=T,R, z=ES,DS,ESS,DSS vo verzii staršej ako 1.270
MELSEC iQ-F FX5UC-xMy/z x=32,64,96, y=T,R, z=D,DS vo verzii staršej ako 1.270
MELSEC iQ-F FX5UC-32MT/DS-TS, FX5UC-32MT/DSS-TS, FX5UC-32MR/DS-TS vo verzii staršej ako 1.270
MELSEC iQ-F FX5UJ-xMy/z x=24,40,60, y=T,R, z=ES,ESS vo verzii staršej ako 1.030

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

https://us-cert.cisa.gov/ics/advisories/icsa-22-139-01

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 8.5
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

NVIDIA GPU Display Driver - viacero bezpečnostných zraniteľností

Popis

Spoločnosť NVIDIA vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa eskalovať svoje privilégiá a následne vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

16.05.2022

CVE

-

Zasiahnuté systémy

GeForce driver R510 pre Windows vo verzii staršej ako 512.77
Studio driver R510 pre Windows všetky verzie
NVIDIA RTX/QUADRO, NVS driver R510 pre Windows vo verzii staršej ako 512.78
NVIDIA RTX/QUADRO, NVS driver R740 pre Windows vo verzii staršej ako 473.47
Tesla, driver R510 pre Windows všetky verzie
Tesla, driver R470 pre Windows vo verzii staršej ako 473.47
Tesla, driver R450 pre Windows vo verzii staršej ako 453.51
GeForce driver R510 pre Linux vo verzii staršej ako 510.73.05
GeForce driver R470 pre Linux vo verzii staršej ako 470.129.06
GeForce driver R390 pre Linux vo verzii staršej ako 390.151
GeForce driver R510 pre Linux všetky verzie
GeForce driver R470 pre Linux vo verzii staršej ako 470.129.06
GeForce driver R450 pre Linux vo verzii staršej ako 450.191.01

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
v prípade Tesla driver R510 pre Windows a GeForce driver R510 pre Linux odporúčame sledovať stránku výrobcu a po vydaní bezpečnostných záplat 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://nvidia.custhelp.com/app/answers/detail/a_id/5353 https://www.bleepingcomputer.com/news/security/nvidia-fixes-ten-vulnerabilities-in-windows-gpu-display-drivers/

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

Identifikátor

TatsuBuilder pluginu pre Wordpress - bezpečnostná zraniteľnosť

Popis

Vývojári pluginu TatsuBuilder vydali bezpečnostnú aktualizáciu svojho produktu, opravujúcu bezpečnostnú zraniteľnosť ktorá umožňuje vzdialenému, neautentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

17.05.2022

CVE

CVE-2021-25094

Zasiahnuté systémy

TatsuBuilder plugin pre WordPress vo verzii staršej ako 3.3.13

Následky

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

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.
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-2021-25094#vulnCurrentDescriptionTitle
https://www.wordfence.com/blog/2022/05/millions-of-attacks-target-tatsu-builder-plugin/

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

Identifikátor

Linux Kernel - bezpečnostná zraniteľnosť

Popis

Vývojári jadra operačného systému Linux vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa eskalovať svoje privilégiá a získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

20.05.2022

CVE

CVE-2022-1729

Zasiahnuté systémy

Linux Kernel vo verzii staršej ako v5.18

Následky

Eskalácia privilégií a následné 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://exchange.xforce.ibmcloud.com/vulnerabilities/227038
https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.1**
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

NETGEAR BR200 a BR500 - viacero bezpečnostných zraniteľností

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnostiach produktov BR200 a BR500 od spoločnosti NETGEAR.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorenej webovej stránky eskalovať svoje privilégiá a následne získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť čiastočné zneprístupnenie služby.

Dátum prvého zverejnenia varovania

20.05.2022

CVE

-

Zasiahnuté systémy

BR200 - všetky verzie
BR500 - všetky verzie

Následky

Neoprávnený prístup do systému a úplné narušenie dôvernosti, integrity a čiastočné narušenie dostupnosti systému

Odporúčania

Na uvedenú zraniteľnosť podľa výrobcu kvôli technickým limitáciám nebude vydaná bezpečnostná záplata, administrátorom preto odporúčame sledovať stránku výrobcu a prípadne vykonať výmenu zasiahnutých systémov za novšie odporúčané výrobcom.
Detailné inštrukcie môžete nájsť na webovej adrese: https://kb.netgear.com/000064712/Security-Advisory-for-Multiple-Security-Vulnerabilities-on-BR200-and-BR500-PSV-2021-0286
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.

Zdroje

https://kb.netgear.com/000064712/Security-Advisory-for-Multiple-Security-Vulnerabilities-on-BR200-and-BR500-PSV-2021-0286
https://www.helpnetsecurity.com/2022/05/20/two-business-grade-netgear-vpn-routers-have-security-vulnerabilities-that-cant-be-fixed/

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.0**
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

BIND 9 - bezpečnostná zraniteľnosť

Popis

Konzorcium ISC vydala bezpečnostnú aktualizáciu na svoj produkt BIND 9, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej požiadavky spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

18.05.2022

CVE

CVE-2022-1183

Zasiahnuté systémy

BIND vo verzii staršej ako 9.18.3 (aktuálna stabilná verzia)
BIND vo verzii staršej ako 9.19.1 (development verzia)

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://kb.isc.org/docs/cve-2022-1183