BEZPEČNOSTNÝ BULLETIN

Týždeň 21. 04. 2021 - 27. 04. 2021

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:
01439/2020/SK-CERT-401

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 vydala bezpečnostné aktualizácie na produkty Firefox 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

19.04.2021

CVE

CVE-2021-23994, CVE-2021-23995, CVE-2021-23996, CVE-2021-23997, CVE-2021-23998, CVE-2021-23999, CVE-2021-24000, CVE-2021-24001, CVE-2021-24002, CVE-2021-29943, CVE-2021-29944, CVE-2021-29946, CVE-2021-29947, CVE-2021-29948

Zasiahnuté systémy

Mozilla Thunderbird vo verzii staršej ako 78.10
Mozilla Firefox ESR vo verzii staršej ako 78.10
Mozilla Firefox vo verzii staršej ako 88

Následky

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

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/mfsa2021-16/
https://www.mozilla.org/en-US/security/advisories/mfsa2021-15/
https://www.mozilla.org/en-US/security/advisories/mfsa2021-14/
https://threatpost.com/mozilla-fixes-firefox-flaw/165501/
https://exchange.xforce.ibmcloud.com/vulnerabilities/200185

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:
01439/2020/SK-CERT-401

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.4**
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Horner Automation Cscape - bezpečnostné zraniteľnosti

Popis

Spoločnosť Horner Automation vydala bezpečnostnú aktualizáciu na svoj produkt Cscape, ktorá opravuje dve bezpečnostné zraniteľnosti.
Bezpečnostná zraniteľnosť je spôsobená nedostatočným overovaním používateľských vstupov a umožňuje lokálnemu, neautentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

22.04.2021

CVE

CVE-2021-22678, CVE-2021-22682

Zasiahnuté systémy

Cscape všetky verzie staršie ako 9.90 SP4

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://us-cert.cisa.gov/ics/advisories/icsa-21-112-01

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

Identifikátor

Rockwell Automation Stratix Switches - bezpečnostné zraniteľnosti

Popis

Spoločnosť Rockwell Automation vydala bezpečnostné aktualizácie na svoje produkty Stratix Switches, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s používateľskými právomocami eskalovať svoje privilégiá a následne vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

20.04.2021

CVE

CVE-2021-1220, CVE-2021-1352, CVE-2021-1356, CVE-2021-1392, CVE-2021-1403, CVE-2021-1442, CVE-2021-1443, CVE-2021-1452

Zasiahnuté systémy

Stratix 5800 vo verzii staršej ako 17.04.01
Stratix 8000 vo verzii staršej ako 15.2(7)E3 (vrátane)
Stratix 5700 vo verzii staršej ako 15.2(7)E3 (vrátane)
Stratix 5410 vo verzii staršej ako 15.2(7)E3 (vrátane)
Stratix 5400 vo verzii staršej ako 15.2(7)E3 (vrátane)

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 verzií Stratix 8000, 5700, 5410, 5400 administrátorom odporúčame realizovať odporúčania zverejnené na adrese https://us-cert.cisa.gov/ics/advisories/icsa-21-110-02
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://us-cert.cisa.gov/ics/advisories/icsa-21-110-02

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.8**
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, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje lokálnemu, autentifikovanému útočníkovi s používateľskými právomocami získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

21.04.2021

CVE

CVE-2021-1080,CVE-2021-1074,CVE-2021-1075,CVE-2021-1076,CVE-2021-1077,CVE-2021-1078,CVE-2021-1079,CVE-2021-1081,CVE-2021-1082,CVE-2021-1083,CVE-2021-1084,CVE-2021-1085,CVE-2021-1086,CVE-2021-1087

Zasiahnuté systémy

NVIDIA GeForce R465 vo verzii staršej ako 466.11
NVIDIA GeForce R460 vo verzii staršej ako 462.31
NVIDIA RTX/Quadro R465, NVS vo verzii staršej ako 466.11
NVIDIA RTX/Quadro R460, NVS vo verzii staršej ako 462.31
NVIDIA RTX/Quadro R450, NVS vo verzii staršej ako 452.96
NVIDIA RTX/Quadro R390, NVS vo verzii staršej ako 392.65
NVIDIA Tesla R460 vo verzii staršej ako 462.31
NVIDIA Tesla R450 vo verzii staršej ako 452.96
NVIDIA Tesla R418 vo verzii staršej ako 427.33
NVIDIA vGPU software pre Windows (guest driver) vo verzii staršej ako 12.2
NVIDIA vGPU software pre Linux (guest driver) vo verzii staršej ako 11.4

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme
Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Administrátorom odporúčame limitovať prístup k administratívnemu rozhraniu a jeho funkciám zavedením zoznamu pre riadenie prístupov (ACL).
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://nvidia.custhelp.com/app/answers/detail/a_id/5172

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

Identifikátor

VMware NSX-T produkt - bezpečnostná zraniteľnosť

Popis

Spoločnosť VMware vydala bezpečnostnú aktualizáciu na svoj produkt NSX-T, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi prostredníctvom zasielania špeciálne vytvorenej požiadavky eskalovať svoje privilégiá a následne vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

19.04.2021

CVE

CVE-2021-21981

Zasiahnuté systémy

VMware NSX-T vo verzii staršej ako 3.1.2

Následky

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

Odporúčania

Administrátorom 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://exchange.xforce.ibmcloud.com/vulnerabilities/200183
https://www.vmware.com/security/advisories/VMSA-2021-0006.html

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

Identifikátor

Authelia produkt - bezpečnostná zraniteľnosť

Popis

Vývojári programu Authelia vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorenej URL adresy vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

21.04.2021

CVE

CVE-2021-29456

Zasiahnuté systémy

Authelia vo verzii staršej ako 4.28.0

Následky

Neoprávnená zmena v systéme

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.

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/200535
https://github.com/authelia/authelia
https://github.com/authelia/authelia/security/advisories/GHSA-36f2-fcrx-fp4j