BEZPEČNOSTNÝ BULLETIN

Týždeň 30. 11. 2022 - 06. 12. 2022

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	ABB Zenon - tri bezpečnostné zraniteľnosti	Vysoká	**8.8**
02.	NVIDIA produkty - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
03.	Sinatra - bezpečnostná zraniteľnosť	Vysoká	**8.8**
04.	Hitachi Energy MicroSCADA a IED - dve bezpečnostné zraniteľnosti	Vysoká	**8.8**
05.	Omron - tri bezpečnostné zraniteľnosti	Vysoká	**8.6**
06.	Notebooky Acer - bezpečnostná zraniteľnosť	Vysoká	**8.2**
07.	HPE OneView - bezpečnostná zraniteľnosť	Vysoká	**7.8**
08.	FlyingPress WP plugin - bezpečnostná zraniteľnosť	Vysoká	**7.6**
09.	MOXA UC Series - bezpečnostná zraniteľnosť	Vysoká	**7.6**
10.	Apache Fineract - bezpečnostná zraniteľnosť	Vysoká	**7.5**

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-959

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

Identifikátor

ABB Zenon - tri bezpečnostné zraniteľnosti

Popis

Spoločnosť ABB vydala bezpečnostnú aktualizáciu na svoju platformu Zenon, ktorá opravuje tri bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi extrahovať prístupové heslo do SQL databázy konfiguračného nástroja Zenon, tým získať neoprávnený prístup do systému a následne získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

29.11.2022

CVE

CVE-2022-34836, CVE-2022-34837, CVE-2022-34838

Zasiahnuté systémy

ABB Zenon vo verzii staršej ako 8.20

Následky

Neoprávnený prístup do systému
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.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.
Administrátorom odporúčame limitovať prístup k zariadeniu pomocou nastavení prvkov bezpečnostnej architektúry.

Zdroje

https://search.abb.com/library/Download.aspx?DocumentID=2NGA001479&LanguageCode=en&DocumentPartId=&Action=Launch&_ga=2.210195794.655292894.1669797442-1784065056.1661159789

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

Identifikátor

NVIDIA produkty - 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 lokálnemu, autentifikovanému útočníkovi s právomocami používateľa zneužitím bližšie nešpecifikovanej zraniteľnosti v užívateľskom móde vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

28.11.2022

CVE

CVE-2022-34670, CVE-2022-34671, CVE-2022-34672, CVE-2022-34673, CVE-2022-34674, CVE-2022-34675, CVE-2022-34676, CVE-2022-34677, CVE-2022-34678, CVE-2022-34679, CVE-2022-34680, CVE-2022-34681, CVE-2022-34682, CVE-2022-34683, CVE-2022-34684, CVE-2022-42254, CVE-2022-42255, CVE-2022-42256, CVE-2022-42257, CVE-2022-42258, CVE-2022-42259, CVE-2022-42260, CVE-2022-42261, CVE-2022-42262, CVE-2022-42263, CVE-2022-42264, CVE-2022-42265, CVE-2022-42266

Zasiahnuté systémy

NVIDIA GPU Display Driver, NVIDIA VGPU, NVIDIA GPU LINUX Display Driver, NVIDIA CLOUD GAMING guest driver v rôznych verziách. Presnú špecifikáciu jednotlivých zasiahnutých produktov nájdete na odkaze v sekcii ZDROJE.

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://nvidia.custhelp.com/app/answers/detail/a_id/5415

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

Identifikátor

Sinatra - bezpečnostná zraniteľnosť

Popis

Vývojári frameworku Sinatra 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 vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

01.12.2022

CVE

CVE-2022-45442

Zasiahnuté systémy

Sinatra vo verzii staršej ako 2.2.3, 3.0.4

Následky

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

Odporúčania

Odporúčame uistiť sa, či Vaše aplikácie nevyužívajú predmetný framework 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://www.redpacketsecurity.com/sinatra-code-execution-cve-2022-45442/

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

Identifikátor

Hitachi Energy MicroSCADA a IED - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť Hitachi Energy vydala bezpečnostnú aktualizáciu na svoje produkty MicroSCADA a IED, ktoré opravujú dve bezpečnostné zraniteľnosti.
Bezpečnostná zraniteľnosť spočíva v nedostatočneom overovaní používateľských vstupov a umožňuje lokálnemu, autentifikovanému útočníkovi s právami používateľa vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

02.12.2022

CVE

CVE-2022-2513, CVE-2022-3388

Zasiahnuté systémy

Hitachi Energy MicroSCADA Pro/X vo verzii staršej ako SYS600 10.4 (vrátane)
Hitachi Energy MicroSCADA Pro/X vo verzii staršej ako SYS600 9.4 FP2 Hotfix 4 (vrátane)
Hitachi Energy PCM600 vo verzii staršej ako 2.11 Hotfix 20220923
Hitachi Energy 670 Connectivity Package vo verziách 3.0 do 3.4.1 (vrátane)
Hitachi Energy 650 Connectivity Package vo verziách 1.3 do 2.4.1 (vrátane)
Hitachi Energy SAM600-IO Connectivity Package vo verziách 1.0 do 1.2 (vrátane)
Hitachi Energy GMS600 Connectivity Package vo verziách 1.3 do 1.3.1 (vrátane)
Hitachi Energy PWC600 Connectivity Package vo verziách 1.1 do 1.3 (vrátane)

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov a postupovať podľa inštrukcií výrobcu, ktoré sú dostupné na webových adresách v časti ZDROJE.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.
Administrátorom odporúčame limitovať prístup k administratívnemu rozhraniu a jeho funkciám zavedením zoznamu pre riadenie prístupov (ACL).
Po odstránení zraniteľností, ktoré mohli spôsobiť vykonanie škodlivého kódu 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://search.abb.com/library/Download.aspx?DocumentID=8DBD000120&LanguageCode=en&DocumentPartId=&Action=Launch https://search.abb.com/library/Download.aspx?DocumentID=8DBD000123&LanguageCode=en&DocumentPartId=&Action=Launch&elqaid=4293&elqat=1

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

Identifikátor

Omron - tri bezpečnostné zraniteľnosti

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnostiach produktov Omron PLC CJ, CS a NX1P2 series.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi neoprávnený prístup do zariadenia a následné úplné narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

29.11.2022

CVE

CVE-2019-13533, CVE-2019-18259, CVE-2019-18269

Zasiahnuté systémy

Omron PLC CJ series vo všetkých verziách
Omron PLC CS series vo všetkých verziách
Omron PLC NX1P2 series vo všetkých verziách

Následky

Úplné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Pri produktoch, pre ktoré ešte neboli vydané bezpečnostné záplaty, odporúčame zraniteľnosti mitigovať podľa odporúčaní od výrobcu, sledovať stránky výrobcu a po vydaní príslušných záplat systémy aktualizovať.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.
Administrátorom odporúčame filtrovať sieťovú komunikáciu bezpečnostnými prvkami sieťovej infraštruktúry ako aj zablokovanie nepotrebného vzdialeného prístupu na FINS port (predvolene 9600).
Ak je vzdialený prístup potrebný, použite virtuálnu súkromnú sieť (VPN).

Zdroje

https://www.cisa.gov/uscert/ics/advisories/icsa-19-346-02
https://www.omron-cxone.com/security/2019-12-06_PLC_EN.pdf

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

Identifikátor

Notebooky Acer - bezpečnostná zraniteľnosť

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnosti notebookov Acer.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami administrátora prostredníctvom úpravy premenných NVRAM vypnúť funkciu Secure Boot, nahrať vlastný bootloader a vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

28.11.2022

CVE

CVE-2022-4020

Zasiahnuté systémy

Aspire A315-22, A115-21 a A315-22G
Extensa EX215-21 a EX215-21G

Následky

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

Odporúčania

Na uvedenú zraniteľnosť v súčasnosti nebola vydaná bezpečnostná záplata, administrátorom preto odporúčame sledovať stránku výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu zasiahnutých systémov.
Bezpečnostná záplata má byť obsiahnutá v aktualizácii UEFI BIOS, preto používateľom odporúčame nainštalovať aktualizácie systému UEFI BIOS z webových stránok výrobcu v momente keď budú dostupné pre ich konkrétne elektronické zariadenie.
V prípade, že prevádzkujete fyzické servery s operačným systémom Linux, uistite sa, že máte nainštalovaný balík intel-microcode. Na BSD systémoch môžete použiť balík cpupdate.
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-2022-4020
https://cybernews.com/news/acer-flaw-malware-boot-process/
https://community.acer.com/en/kb/articles/15520-security-vulnerability-regarding-vulnerability-that-may-allow-changes-to-secure-boot-settings

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

Identifikátor

HPE OneView - bezpečnostná zraniteľnosť

Popis

Spoločnosť Hewlett Packard Enterprise vydala bezpečnostnú aktualizáciu pre svoj softvér na správu siete a systémov OneView, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa bližšie nepopísaným spôsobom narušiť dôvernosť, integritu a dostupnosť systému.
Na zneužitie tejto zraniteľnosti musí byť pre OneView nastavený prihlasovací prístup k externým repozitárom.

Dátum prvého zverejnenia varovania

28.11.2022

CVE

CVE-2022-28625

Zasiahnuté systémy

HPE OneView vo verzii staršej ako 7.0
HPE OneView vo verzii staršej ako 6.60.01

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://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbgn04304en_us

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.6
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

FlyingPress WP plugin - bezpečnostná zraniteľnosť

Popis

Vývojári pluginu FlyingPress pre webový redakčný systém WordPress vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa zneužiť save_config funkciu a vykonať neoprávnené zmeny v systéme a zneprístupnenie služby.

Dátum prvého zverejnenia varovania

28.11.2022

CVE

-

Zasiahnuté systémy

FlyingPress WP plugin vo verzii staršej ako 3.9.7

Následky

Neoprávnená zmena v systéme
Zneprístupnenie služby

Odporúčania

Odporúčame uistiť sa, či Vaše webové stránky a aplikácie založené na redakčnom systéme WordPress nevyužívajú predmetný plugin v zraniteľnej verzii. V prípade, že áno, zabezpečte aktualizáciu redakčného systému a všetkých používaných pluginov na aktuálne verzie bez známych bezpečnostných zraniteľností.

Zdroje

https://blog.nintechnet.com/wordpress-flyingpress-plugin-fixed-broken-access-control-vulnerability/
https://patchstack.com/database/vulnerability/flying-press/wordpress-flyingpress-premium-plugin-3-9-6-arbitrary-settings-update-vulnerability-to-stored-cross-site-scripting-xss

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.6
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

MOXA UC Series - bezpečnostná zraniteľnosť

Popis

Spoločnosť MOXA vydala bezpečnostné aktualizácie na svoje produkty UC Series, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi s fyzickým prístupom k zariadeniu získať úplnú kontrolu nad systémom.

Dátum prvého zverejnenia varovania

29.11.2022

CVE

CVE-2022-3086

Zasiahnuté systémy

MOXA UC-8580 Series vo verziách od V1.1
MOXA MOXAUC-8540 Series vo verziách od V1.0 do V1.2
MOXA UC-8410A Series vo verziách od V2.2
MOXA UC-8200 Series vo verziách od V1.0 do V2.4
MOXA UC-8100A-ME-T Series vo verziách od V1.0 do V1.1
MOXA UC-8100 Series vo verziách od V1.2 do V1.3
MOXA UC-5100 Series vo verziách od V1.2
MOXA UC-3100 Series vo verziách od V1.2 do V2.0
MOXA UC-2100 Series vo verziách od V1.3 do V1.5
MOXA UC-2100-W Series vo verziách od V1.3 do V1.5

Následky

Úplná kontrola nad systémom

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov, ktorá by mala byť dostupná na webstránke výrobcu po prihlásení sa na adrese https://www.moxa.com/en/membership/sign-in?returnurl=%2fen%2fsupport%2ftechnical-support
Administrátorom odporúčame limitovať prístup k administratívnemu rozhraniu a jeho funkciám zavedením zoznamu pre riadenie prístupov (ACL).
Po odstránení zraniteľností, ktoré mohli spôsobiť získanie úplnej kontroly nad systémom 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.moxa.com/en/membership/sign-in?returnurl=%2fen%2fsupport%2ftechnical-support https://www.cisa.gov/uscert/ics/advisories/icsa-22-333-04

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

Identifikátor

Apache Fineract - bezpečnostná zraniteľnosť

Popis

Vývojári platformy Fineract vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom podvrhnutia špeciálne vytvoreného súboru vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

29.11.2022

CVE

CVE-2022-44635

Zasiahnuté systémy

Apache Fineract vo verzii staršej ako 1.8.1

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 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.
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/241056