BEZPEČNOSTNÝ BULLETIN

Týždeň 01. 02. 2023 - 07. 02. 2023

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	TRENDnet TEW-652BRP - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
02.	NVIDIA GeForce Experience - viacero bezpečnostných zraniteľností	Vysoká	**8.2**
03.	Delta Electronics DOPSoft - dve bezpečnostné zraniteľnosti	Vysoká	**7.8**
04.	VMware Workstation - bezpečnostná zraniteľnosť	Vysoká	**7.8**
05.	Hitachi Storage Plug-in - dve bezpečnostné zraniteľnosti	Vysoká	**7.6**
06.	Wattbox WB-300-IP-3 - viacero bezpečnostných zraniteľností	Vysoká	**7.5**
07.	F5 BIG-IP- viacero bezpečnostných zraniteľností	Vysoká	**7.5**
08.	Django - bezpečnostná zraniteľnosť	Vysoká	**7.5**
09.	Cisco produkty - viacero bezpečnostných zraniteľností	Vysoká	**7.2**
10.	Huawei AILife - dve bezpečnostné zraniteľnosti	Vysoká	**7.0**

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-1020

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

Identifikátor

TRENDnet TEW-652BRP - viacero bezpečnostných zraniteľností

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnostiach routera TEW-652BRP.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom injekcie špeciálne upravených príkazov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.
Na uvedenú zraniteľnosť je v súčasnosti voľne dostupný Proof-of-Concept kód a zraniteľnosť je aktívne zneužívaná útočníkmi.

Dátum prvého zverejnenia varovania

01.02.2023

CVE

CVE-2023-0611, CVE-2023-0612, CVE-2023-0613, CVE-2023-0617, CVE-2023-0618, CVE-2023-0637

Zasiahnuté systémy

TRENDnet TEW-652BRP s firmvérom vo verzii staršej ako 3.04B01 (vrátane)

Následky

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

Odporúčania

Administrátorom 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://nvd.nist.gov/vuln/detail/CVE-2023-0611
https://exchange.xforce.ibmcloud.com/vulnerabilities/246225
https://exchange.xforce.ibmcloud.com/vulnerabilities/246213
https://exchange.xforce.ibmcloud.com/vulnerabilities/246218
https://exchange.xforce.ibmcloud.com/vulnerabilities/246221
https://exchange.xforce.ibmcloud.com/vulnerabilities/246222
https://exchange.xforce.ibmcloud.com/vulnerabilities/246224

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

Identifikátor

NVIDIA GeForce Experience - viacero bezpečnostných zraniteľností

Popis

Spoločnosť NVIDIA vydala bezpečnostnú aktualizáciu na svoj produkt GeForce Experience, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi vykonať neoprávnené zmeny v systéme a zneprístupnenie služby.

Dátum prvého zverejnenia varovania

30.01.2023

CVE

CVE-2022-42291, CVE-2022-31611, CVE-2022-42292

Zasiahnuté systémy

GeForce Experience vo verzii staršej ako 3.27.0.112

Následky

Neoprávnená zmena v systéme
Zneprístupnenie služby
Vykonanie škodlivého kódu

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://nvidia.custhelp.com/app/answers/detail/a_id/5384

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

Identifikátor

Delta Electronics DOPSoft - dve bezpečnostné zraniteľnosti

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnostiach HMI editovacieho softvéru DOPSoft. Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

31.01.2023

CVE

CVE-2023-0123, CVE-2023-0124

Zasiahnuté systémy

Delta Electronics DOPSoft vo všetkých verziách

Následky

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

Odporúčania

Vzhľadom na to, že produkt už nie je udržiavaný, výrobca odporúča prejsť na produkt s platnou podporou - DIAScreen vo verzii staršej ako 1.3.0.

Zdroje

https://www.cisa.gov/uscert/ics/advisories/icsa-23-031-01

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

Identifikátor

VMware Workstation - bezpečnostná zraniteľnosť

Popis

Spoločnosť VMware vydala bezpečnostnú aktualizáciu na svoj hypervízor Workstation, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa vo virtuálnom stroji vymazať ľubovoľný súbor z počítača s nainštalovaným VMWare Workstation a spôsobiť narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

02.02.2023

CVE

CVE-2023-20854

Zasiahnuté systémy

VMware Workstation vo verzii staršej ako 17.0.1

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://www.vmware.com/security/advisories/VMSA-2023-0003.html

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

Identifikátor

Hitachi Storage Plug-in - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť Hitachi vydala bezpečnostnú aktualizáciu na svoj Storage Plug-in pre VMware vCenter, ktorá opravuje dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa eskalovať svoje privilégiá a spôsobiť narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

30.01.2023

CVE

CVE-2022-4041, CVE-2022-4441

Zasiahnuté systémy

Hitachi Storage Plug-in for VMware vCenter vo verzii staršej ako 04.9.1.

Následky

Eskalácia privilégií
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/245937
https://www.hitachi.com/products/it/software/security/info/vuls/hitachi-sec-2023-103/index.html

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

Identifikátor

Wattbox WB-300-IP-3 - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Snap One vydala bezpečnostnú aktualizáciu na svoju prepäťovú ochranu Wattbox WB-300-IP-3, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom brute force útoku získať neoprávnený prístup do sysétmu a následne vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

26.01.2023

CVE

CVE-2023-22315, CVE-2023-22389, CVE-2023-23582, CVE-2023-24020

Zasiahnuté systémy

Snap One Wattbox WB-300-IP-3 vo verzii staršej ako WB10.B929

Následky

Neoprávnený prístup do systému
Neoprávnený prístup k citlivým informáciám
Znemožnenie služby
Vykonanie škodlivého kódu

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu. Administrátorom odporúčame filtrovať sieťovú komunikáciu bezpečnostnými prvkami sieťovej infraštruktúry. Ak je potrebný vzdialený prístup, použite virtuálnu súkromnú sieť (VPN).

Zdroje

https://www.cisa.gov/uscert/ics/advisories/icsa-23-026-03

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

Identifikátor

F5 BIG-IP- viacero bezpečnostných zraniteľností

Popis

Spoločnosť F5 vydala bezpečnostné aktualizácie na produkty BIG-IP a BIG-IP SPK, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia 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

01.02.2023

CVE

CVE-2023-22281, CVE-2023-22283, CVE-2023-22302, CVE-2023-22323, CVE-2023-22326, CVE-2023-22340, CVE-2023-22341, CVE-2023-22358, CVE-2023-22374, CVE-2023-22418, CVE-2023-22422, CVE-2023-22657, CVE-2023-22664, CVE-2023-22842, CVE-2023-23552, CVE-2023-23555

Zasiahnuté systémy

BIG-IP vo verzii staršej ako 14.1.5.3 a 15.1.8
BIG-IP SPK vo verzii staršej ako 1.6

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje
https://my.f5.com/manage/s/article/K24572686
https://exchange.xforce.ibmcloud.com/vulnerabilities/246185
https://exchange.xforce.ibmcloud.com/vulnerabilities/246156
https://exchange.xforce.ibmcloud.com/vulnerabilities/246157
https://exchange.xforce.ibmcloud.com/vulnerabilities/246160
https://exchange.xforce.ibmcloud.com/vulnerabilities/246161
https://exchange.xforce.ibmcloud.com/vulnerabilities/246163
https://exchange.xforce.ibmcloud.com/vulnerabilities/246164
https://exchange.xforce.ibmcloud.com/vulnerabilities/246165
https://exchange.xforce.ibmcloud.com/vulnerabilities/246166
https://exchange.xforce.ibmcloud.com/vulnerabilities/246167
https://exchange.xforce.ibmcloud.com/vulnerabilities/246183
https://exchange.xforce.ibmcloud.com/vulnerabilities/246184
https://exchange.xforce.ibmcloud.com/vulnerabilities/246199
https://exchange.xforce.ibmcloud.com/vulnerabilities/246200
https://exchange.xforce.ibmcloud.com/vulnerabilities/246201
https://exchange.xforce.ibmcloud.com/vulnerabilities/246202

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

Identifikátor

Django - bezpečnostná zraniteľnosť

Popis

Vývojári frameworku Django vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutej špeciálne vytvorených "Accept-Language" hlavičiek spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

01.02.2023

CVE

CVE-2023-23969

Zasiahnuté systémy

Django vo verzii staršej ako 4.1.6
Django vo verzii staršej ako 4.0.9
Django vo verzii staršej ako 3.2.17

Následky

Zneprístupnenie služby

Odporúčania

Odporúčame uistiť sa, či Vaše webové aplikácie nie sú založené na frameworku Django v zraniteľných verziách. V prípade, že áno, administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://seclists.org/oss-sec/2023/q1/72
https://exchange.xforce.ibmcloud.com/vulnerabilities/246168

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.2
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Cisco produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Cisco vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť sa nachádza v aplikácii Cisco IOx, spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami administrátora prostredníctvom podvrhnutia špeciálne vytvoreného aktivačného súbora vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

01.02.2023

CVE

CVE-2023-20021, CVE-2023-20022, CVE-2023-20023, CVE-2023-20030, CVE-2023-20040, CVE-2023-20068, CVE-2023-20073, CVE-2023-20076

Zasiahnuté systémy

Cisco ISE
Cisco NSO
Cisco Prime Infrastructure Software
Cisco zariadenia prevádzkujúce Cisco IOS XE softvér ak majú spustenú funkcionalitu Cisco IOx a nepodporujú natívny docker
RV340 Dual WAN Gigabit VPN Routers
RV340W Dual WAN Gigabit Wireless-AC VPN Routers
RV345 Dual WAN Gigabit VPN Routers
RV345P Dual WAN Gigabit POE VPN Routers
Presnú špecifikáciu jednotlivých zasiahnutých produktov nájdete na odkazoch v sekcii ZDROJE

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Administrátorom odporúčame filtrovať sieťovú komunikáciu bezpečnostnými prvkami sieťovej infraštruktúry. Ak je potrebný vzdialený prístup, použite virtuálnu súkromnú sieť (VPN).

Zdroje
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-pi-xss-PU6dnfD9
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-os-injection-pxhKsDM
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-xxe-inj-GecEHY58
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv-afu-EXxwA65V
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-8whGn5dL
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nso-path-trvsl-zjBeMkZg

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

Identifikátor

Huawei AILife - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť Huawei vydala bezpečnostnú aktualizáciu na svoj smart home softvér AILife, ktorá opravuje dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zaslania špeciálne vytvorenej požiadavky eskalovať svoje privilégiá a následne získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

01.02.2023

CVE

CVE-2022-48283

Zasiahnuté systémy

Huawei HarmonyOS AILife Solution 6.0 HiLink AI Life vo verzii staršej ako 12.0.3.305

Následky

Úplné narušenie dôvernosti, integrity a dostupnosti systému
Eskalácia privilégií

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/246159
https://exchange.xforce.ibmcloud.com/vulnerabilities/246158