BEZPEČNOSTNÝ BULLETIN

Týždeň 20. 12. 2023 - 26. 12. 2023

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Chrome - bezpečnostná zraniteľnosť	Vysoká	**8.8**
02.	Inductive Automation Ignition - bezpečnostná zraniteľnosť	Vysoká	**8.8**
03.	D-Link G416 - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
04.	Honeywell Saia PG5 Controls Suite - viacero zero day bezpečnostných zraniteľností	Vysoká	**8.8**
05.	ioLogik E1200 Series Web Server - dve bezpečnostné zraniteľnosti	Vysoká	**8.8**
06.	NETGEAR ProSAFE NMS300 - bezpečnostná zraniteľnosť	Vysoká	**8.8**
07.	Mozilla produkty - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
08.	Subnet Solutions PowerSYSTEM Center - bezpečnostná zraniteľnosť	Vysoká	**7.8**
09.	Kofax Power PDF - viacero zero day bezpečnostných zraniteľností	Vysoká	**7.8**
10.	Open Design Alliance Drawing SDK - tri bezpečnostné zraniteľnosti	Vysoká	**7.8**
11.	NVIDIA Triton Inference Server - bezpečnostná zraniteľnosť	Vysoká	**7.5**
12.	HPE Unified OSS Console a Integrated Lights-Out - dve bezpečnostné zraniteľnosti	Vysoká	**7.5**
13.	GitHub Enterprise Server - viacero bezpečnostných zraniteľností	Vysoká	**7.5**
14.	BlueZ - viacero zero day bezpečnostných zraniteľností	Vysoká	**7.1**
15.	EFACEC UC 500 - viacero bezpečnostných zraniteľností	Stredná	**6.3**

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-1452

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

Identifikátor

Chrome - bezpečnostná zraniteľnosť

Popis

Spoločnosť Google vydala bezpečnostnú aktualizáciu na svoj produkt Chrome, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov v rámci komponentu WebRTC 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

20.12.2023

CVE

CVE-2023-7024

Zasiahnuté systémy

Chrome pre Mac a Linux vo verzii staršej ako 120.0.6099.129
Chrome pre Windows vo verzii staršej ako 120.0.6099.129/130

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.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.

Zdroje

https://chromereleases.googleblog.com/2023/12/stable-channel-update-for-desktop_20.html

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

Identifikátor

Inductive Automation Ignition - bezpečnostná zraniteľnosť

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnosti produktu Ignition.
Bezpečnostná zraniteľnosť nachádzajúca sa v triede ModuleInvoke spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zaslania špeciálne vytvorenej požiadavky vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

20.12.2023

CVE

CVE-2023-50218

Zasiahnuté systémy

Inductive Automation Ignition vo všetkých verziách

Následky

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

Odporúčania

Na uvedenú zraniteľnosť v súčasnosti nie sú dostupné aktualizácie. 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.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu. Ak je potrebný vzdialený prístup, použite virtuálnu súkromnú sieť (VPN). Administrátorom odporúčame filtrovať sieťovú komunikáciu bezpečnostnými prvkami sieťovej infraštruktúry.

Zdroje

https://www.zerodayinitiative.com/advisories/ZDI-23-1813/

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

Identifikátor

D-Link G416 - viacero bezpečnostných zraniteľností

Popis

Spoločnosť D-Link vydala bezpečnostnú aktualizáciu na svoj produkt G416, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje útočníkovi nachádzajúcemu sa v rovnakom sieťovom segmente prostredníctvom injekcie špeciálne upravených príkazov vykonať škodlivý kód v kontexte používateľa ROOT s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

12.12.2023

CVE

CVE-2023-50198, CVE-2023-50199, CVE-2023-50200, CVE-2023-50201, CVE-2023-50202, CVE-2023-50203, CVE-2023-50204, CVE-2023-50205, CVE-2023-50206, CVE-2023-50207, CVE-2023-50208, CVE-2023-50209, CVE-2023-50210, CVE-2023-50211, CVE-2023-50212, CVE-2023-50213, CVE-2023-50214, CVE-2023-50215, CVE-2023-50216, CVE-2023-50217

Zasiahnuté systémy

D-Link G416 vo verzii staršej ako v1.09B01HotFix Beta**

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://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10367
https://www.zerodayinitiative.com/advisories/ZDI-23-1814/

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

Identifikátor

Honeywell Saia PG5 Controls Suite - viacero zero day bezpečnostných zraniteľností

Popis

Bezpečnostní výskumníci zverejnili informácie o zero day zraniteľnostiach produktu Saia PG5 Controls Suite.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených súborov alebo webstránky vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.
Zneužitie zraniteľnosti vyžaduje interakciu používateľov.

Dátum prvého zverejnenia varovania

20.12.2023

CVE

CVE-2023-51599, CVE-2023-51600, CVE-2023-51601, CVE-2023-51602, CVE-2023-51603, CVE-2023-51604, CVE-2023-51605

Zasiahnuté systémy

Saia PG5 Controls Suite vo verzii staršej ako V2.3.193 (vrátane)

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému
Neoprávnený prístup k citlivým údajom

Odporúčania

Na uvedené zraniteľnosti v súčasnosti nie sú dostupné bezpečnostné aktualizáciu. 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.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu. Ak je potrebný vzdialený prístup, použite virtuálnu súkromnú sieť (VPN). Administrátorom odporúčame filtrovať sieťovú komunikáciu bezpečnostnými prvkami sieťovej infraštruktúry.

Zdroje
https://www.zerodayinitiative.com/advisories/ZDI-23-1848/
https://www.zerodayinitiative.com/advisories/ZDI-23-1854/
https://www.zerodayinitiative.com/advisories/ZDI-23-1853/
https://www.zerodayinitiative.com/advisories/ZDI-23-1852/
https://www.zerodayinitiative.com/advisories/ZDI-23-1851/
https://www.zerodayinitiative.com/advisories/ZDI-23-1850/
https://www.zerodayinitiative.com/advisories/ZDI-23-1849/

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

Identifikátor

ioLogik E1200 Series Web Server - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť Moxa vydala bezpečnostnú aktualizáciu na svoj webserver ioLogik série E1200, ktorá opravuje dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej požiadavky zrealizovať CSRF (Cross-Site Request Forgery) útok a vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

23.12.2023

CVE

CVE-2023-5961, CVE-2023-5962

Zasiahnuté systémy

ioLogik E1200 Series vo verzii firmvéru staršej ako v3.3 (vrátane) bez aplikovanej bezpečnostnej záplaty

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

Zdroje

https://www.moxa.com/en/support/product-support/security-advisory/mpsa-235250-iologik-e1200-series-web-server-vulnerability

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

Identifikátor

NETGEAR ProSAFE NMS300 - bezpečnostná zraniteľnosť

Popis

Spoločnosť NETGEAR vydala bezpečnostnú aktualizáciu na svoj produkt ProSAFE NMS300, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom injekcie škodlivého skriptu vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.
Zraniteľnosť v súčasnosti nemá pridelený identifikátor CVE.

Dátum prvého zverejnenia varovania

19.12.2023

CVE

-

Zasiahnuté systémy

NMS300 vo verzii staršej ako 1.7.0.31

Následky

Vykonanie škodlivého kódu a 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://kb.netgear.com/000065901/Security-Advisory-for-Stored-Cross-Site-Scripting-on-the-NMS300-PSV-2023-0106
https://exchange.xforce.ibmcloud.com/vulnerabilities/275387
https://www.zerodayinitiative.com/advisories/ZDI-23-1847/

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 vydala bezpečnostné aktualizácie na svoje portfólio produktov, 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

19.12.2023

CVE

CVE-2023-50761, CVE-2023-50762, CVE-2023-6135, CVE-2023-6856, CVE-2023-6857, CVE-2023-6858, CVE-2023-6859, CVE-2023-6860, CVE-2023-6861, CVE-2023-6862, CVE-2023-6863, CVE-2023-6864, CVE-2023-6865, CVE-2023-6866, CVE-2023-6867, CVE-2023-6868, CVE-2023-6869, CVE-2023-6870, CVE-2023-6871, CVE-2023-6872, CVE-2023-6873

Zasiahnuté systémy

Firefox vo verzii staršej ako 121
Firefox ESR vo verzii staršej ako 115.6
Thunderbird vo verzii staršej ako 115.6

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.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.

Zdroje

https://www.mozilla.org/en-US/security/advisories/mfsa2023-55/
https://www.mozilla.org/en-US/security/advisories/mfsa2023-54/
https://www.mozilla.org/en-US/security/advisories/mfsa2023-56/
https://exchange.xforce.ibmcloud.com/vulnerabilities/275392

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

Identifikátor

Subnet Solutions PowerSYSTEM Center - bezpečnostná zraniteľnosť

Popis

Spoločnosť Subnet Solutions vydala bezpečnostnú aktualizáciu na svoj produkt PowerSYSTEM Center, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje lokálnemu, 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

19.12.2023

CVE

CVE-2023-6631

Zasiahnuté systémy

PowerSYSTEM Center vo verzii staršej ako 2020 Update 17

Následky

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

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

Zdroje

https://www.cisa.gov/news-events/ics-advisories/icsa-23-353-01

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

Identifikátor

Kofax Power PDF - viacero zero day bezpečnostných zraniteľností

Popis

Bezpečnostní výskumníci zverejnili informácie o zero day zraniteľnostiach produktu Kofax Power PDF.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených súborov alebo webových stránok vykonať škodlivý kód v kontexte prebiehajúceho procesu s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.
Zneužitie zraniteľnosti vyžaduje interakciu používateľov.

Dátum prvého zverejnenia varovania

21.12.2023

CVE

CVE-2023-51597, CVE-2023-51606, CVE-2023-51607, CVE-2023-51608, CVE-2023-51609, CVE-2023-51610, CVE-2023-51611, CVE-2023-51612

Zasiahnuté systémy

Kofax Power PDF vo verzii staršej ako 5.0 (vrátane)

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému
Neoprávnený prístup k citlivým údajom

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.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.

Zdroje

https://www.zerodayinitiative.com/advisories/ZDI-23-1906/
https://www.zerodayinitiative.com/advisories/ZDI-23-1907/
https://www.zerodayinitiative.com/advisories/ZDI-23-1908/
https://www.zerodayinitiative.com/advisories/ZDI-23-1909/
https://www.zerodayinitiative.com/advisories/ZDI-23-1910/
https://www.zerodayinitiative.com/advisories/ZDI-23-1911/
https://www.zerodayinitiative.com/advisories/ZDI-23-1912/
https://www.zerodayinitiative.com/advisories/ZDI-23-1913/

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

Identifikátor

Open Design Alliance Drawing SDK - tri bezpečnostné zraniteľnosti

Popis

Spoločnosť Open Design Alliance vydala bezpečnostnú aktualizáciu na svoj produkt Drawing SDK, ktorá opravuje tri bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom pretečenia zásobníka vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému. Zneužitie zraniteľnosti vyžaduje interakciu používateľov.

Dátum prvého zverejnenia varovania

19.12.2023

CVE

CVE-2023-22669, CVE-2023-22670, CVE-2023-26495, CVE-2023-5179

Zasiahnuté systémy

Drawings SDK vo verzii staršej ako 24.1

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému
Neoprávnený prístup k citlivým údajom

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://www.cisa.gov/news-events/ics-advisories/icsa-23-353-04
https://www.opendesign.com/security-advisories

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

Identifikátor

NVIDIA Triton Inference Server - bezpečnostná zraniteľnosť

Popis

Spoločnosť NVIDIA vydala bezpečnostnú aktualizáciu na svoj produkt Triton Inference Server, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zaslania špeciálne vytvorených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.
Na uvedenú zraniteľnosť je v súčasnosti voľne dostupný Proof-of-Concept kód.

Dátum prvého zverejnenia varovania

18.12.2023

CVE

CVE-2023-31036

Zasiahnuté systémy

NVIDIA Triton Inference Server vo verzii staršej ako 2.40

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému
Zneprístupnenie služby
Neoprávnený prístup k citlivým údajom

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.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.

Zdroje

https://nvidia.custhelp.com/app/answers/detail/a_id/5509
https://huntr.com/bounties/b27148e3-4da4-4e12-95ae-756d33d94687/

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

Identifikátor

HPE Unified OSS Console a Integrated Lights-Out - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť Hewlett Packard Enterprise vydala bezpečnostné aktualizácie na produkty Unified OSS Console a Integrated Lights-Out, ktoré opravujú dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť sa nachádza v produkte iLO 5, spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej požiadavky obísť autentifikáciu a získať neoprávnený prístup k citlivým údajom a vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

19.12.2023

CVE

CVE-2023-50272, CVE-2023-50273

Zasiahnuté systémy

HPE Integrated Lights-Out 5 (iLO 5) vo verzii staršej ako v3.00
HPE Integrated Lights-Out 6 (iLO 6) vo verzii staršej ako v1.55

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme

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=hpesbmu04581en_us
https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04584en_us
https://www.redpacketsecurity.com/hpe-integrated-lights-out-security-bypass-cve-2023-50272/

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

Identifikátor

GitHub Enterprise Server - viacero bezpečnostných zraniteľností

Popis

Spoločnosť GitHub vydala bezpečnostnú aktualizáciu na svoj produkt Enterprise Server, ktorá opravuje viacero bezpečnostných zraniteľností.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej požiadavky získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

21.12.2023

CVE

CVE-2023-46645, CVE-2023-46648, CVE-2023-46649, CVE-2023-51379, CVE-2023-51380, CVE-2023-6690, CVE-2023-6746, CVE-2023-6802, CVE-2023-6803, CVE-2023-6804, CVE-2023-6847

Zasiahnuté systémy

GitHub Enterprise Server vo verzii staršej ako 3.11.1

Následky

Neoprávnený prístup do systému
Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame bezodkladne 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://docs.github.com/en/enterprise-server@3.11/admin/release-notes#3.11.1
https://www.redpacketsecurity.com/github-enterprise-server-security-bypass-cve-2023-6847/
https://nvd.nist.gov/vuln/detail/CVE-2023-6847

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

Identifikátor

BlueZ - viacero zero day bezpečnostných zraniteľností

Popis

Bezpečnostní výskumníci zverejnili informácie o zero day zraniteľnostiach stacku BlueZ.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje útočníkovi nachádzajúcemu sa v rovnakom sieťovom segmente vykonať škodlivý kód v kontexte používateľa ROOT s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.
Zneužitie zraniteľností vyžaduje interakciu používateľov.

Dátum prvého zverejnenia varovania

21.12.2023

CVE

CVE-2023-44431, CVE-2023-51580, CVE-2023-51589, CVE-2023-51592, CVE-2023-51594, CVE-2023-51596

Zasiahnuté systémy

BlueZ vo verzii staršej ako 5.66 (vrátane)

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému
Neoprávnený prístup k citlivým údajom

Odporúčania

Na uvedené zraniteľnosti v súčasnosti nie sú dostupné bezpečnostné aktualizácie. 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://www.zerodayinitiative.com/advisories/ZDI-23-1900/
https://www.zerodayinitiative.com/advisories/ZDI-23-1901/
https://www.zerodayinitiative.com/advisories/ZDI-23-1902/
https://www.zerodayinitiative.com/advisories/ZDI-23-1903/
https://www.zerodayinitiative.com/advisories/ZDI-23-1904/
https://www.zerodayinitiative.com/advisories/ZDI-23-1905/

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 6.3
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

EFACEC UC 500 - viacero bezpečnostných zraniteľností

Popis

Spoločnosť EFACEC vydala bezpečnostnú aktualizáciu na svoj produkt UC 500, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje útočníkovi nachádzajúcemu sa v rovnakom sieťovom segmente zrealizovať MITM (Man In The Middle) útok a získať neoprávnený prístup k citlivým údajom a vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

19.12.2023

CVE

CVE-2023-50703, CVE-2023-50704, CVE-2023-50705, CVE-2023-50706

Zasiahnuté systémy

UC 500E vo verzii staršej ako 10.1.1

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme

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.cisa.gov/news-events/ics-advisories/icsa-23-353-03