BEZPEČNOSTNÝ BULLETIN

Týždeň 18. 01. 2023 - 24. 01. 2023

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-1009

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

Vývojári internetového prehliadača Mozilla vydali bezpečnostné aktualizácie svojich 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

18.01.2023

CVE

CVE-2022-46871, CVE-2022-46877, CVE-2023-23597, CVE-2023-23598, CVE-2023-23599, CVE-2023-23600, CVE-2023-23601, CVE-2023-23602, CVE-2023-23603, CVE-2023-23604, CVE-2023-23605, CVE-2023-23606

Zasiahnuté systémy

Firefox vo verzii staršej ako 109
Firefox ESR vo verzii staršej ako 102.7

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/mfsa2023-01/
https://www.mozilla.org/en-US/security/advisories/mfsa2023-02/
https://www.redpacketsecurity.com/mozilla-firefox-safety-bugs-code-execution-cve-2023-23605/

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

Identifikátor

Sudo - bezpečnostná zraniteľnosť

Popis

Vývojári programu Sudo vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu útočníkovi eskalovať svoje privilégiá a následne získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

16.01.2023

CVE

CVE-2023-22809

Zasiahnuté systémy

Sudo vo verzii staršej ako 1.9.12p2

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://www.synacktiv.com/sites/default/files/2023-01/sudo-CVE-2023-22809.pdf
https://www.sudo.ws/security/advisories/sudoedit_any/
https://vuldb.com/?id.218940

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.3**
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

MS Edge - bezpečnostná zraniteľnosť

Popis

Spoločnosť Microsoft vydala bezpečnostnú aktualizáciu na svoj internetový prehliadač Edge, ktorá opravuje bezpečnostnú zraniteľnosť.
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

12.01.2023

CVE

CVE-2023-21796

Zasiahnuté systémy

Microsoft Edge vo verzii staršej ako 109.0.1518.49

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://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21796
https://exchange.xforce.ibmcloud.com/vulnerabilities/244609

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.1**
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 spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom SQL injekcie získať neoprávnený prístup k citlivým údajom a vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

18.01.2023

CVE

CVE-2022-20806, CVE-2022-20807, CVE-2022-20809, CVE-2023-20010, CVE-2023-20057

Zasiahnuté systémy

Expressway Series vo verzii staršej ako 14.0.7
TelePresence VCS. vo verzii staršej ako 14.0.7
AsyncOS Software pre Cisco Email Security Appliance (ESA)
Unified CM vo verzii staršej ako 12.5(1)SU7 a 14SU3 (Mar 2023)
Unified CM SME vo verzii staršej ako 12.5(1)SU7 a 14SU3 (Mar 2023)

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://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-sql-rpPczR8n
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-url-bypass-WbMQqNJh
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expressway-filewrite-bsFVwueV

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

Identifikátor

Dell EMC PV ME5 - bezpečnostná zraniteľnosť

Popis

Spoločnosť Dell vydala bezpečnostnú aktualizáciu na sieťové úložiská rady ME5, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

17.01.2023

CVE

CVE-2023-23691

Zasiahnuté systémy

Dell PowerVault ME5012, ME5024, a ME5084 vo verziách starších ako ME5.1.1.0.5

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://exchange.xforce.ibmcloud.com/vulnerabilities/245145

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

Identifikátor

X-OPC, X-OTS - bezpečnostná zraniteľnosť

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnostiach produktov X-OPC a X-OTS.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom podvrhnutia špeciálne vytvoreného súboru eskalovať svoje privilégiá a následne získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

11.01.2023

CVE

CVE-2022-4258

Zasiahnuté systémy

HOPCS vo verzii staršej ako 3.56.4
X-OPC A+E vo verzii staršej ako 5.6.1210
X-OPC DA vo verzii staršej ako 5.6.1210
X-OTS vo verzii staršej ako 1.32.550

Následky

Eskalácia privilégií
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 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 filtrovať sieťovú komunikáciu bezpečnostnými prvkami sieťovej infraštruktúry. Ak je potrebný vzdialený prístup, použite virtuálnu súkromnú sieť (VPN).

Zdroje

https://cert.vde.com/en/advisories/VDE-2022-059/

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.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa eskalovať svoje privilégiá, vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

13.01.2023

CVE

CVE-2023-0179

Zasiahnuté systémy

Linux Kernel vo verzii staršej ako commit 696e1a48b1a1

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.

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/244694
https://seclists.org/oss-sec/2023/q1/20

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

Identifikátor

Johnson Controls Metasys ADS/ADX/OAS Servers - bezpečnostná zraniteľnosť

Popis

Spoločnosť Johnson Controls vydala bezpečnostné aktualizácie na svoje produkty Metasys ADS/ADX/OAS Servers, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii mechanizmov autentifikácie a umožňuje lokálnemu, neautentifikovanému útočníkovi získať prístup k prihlasovacím údajom používateľov systému a následne získať úplnú kontrolu nad systémom.

Dátum prvého zverejnenia varovania

12.01.2023

CVE

CVE-2021-36204

Zasiahnuté systémy

Metasys ADS/ADX/OAS 10.X vo verzii staršej ako 10.1.6
Metasys ADS/ADX/OAS 11.X vo verzii staršej ako 11.0.3

Následky

Neoprávnený prístup k citlivým údajom
Úplné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Riadiace systémy a jednotky odporúčame prevádzkovať úplne oddelené od internetu.
Po odstránení zraniteľností, ktoré umožnili útočníkom získať úplnú kontrolu 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.cisa.gov/uscert/ics/advisories/icsa-23-012-06

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

Identifikátor

Trend Micro Maximum Security - bezpečnostná zraniteľnosť

Popis

Spoločnosť Trend Micro vydala bezpečnostnú aktualizáciu na svoj bezpečnostný softvér Maximum Security, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov 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

18.01.2023

CVE

CVE-2022-48191

Zasiahnuté systémy

Trend Micro Maximum Security vo verzii staršej ako 2022 (v17.7) Hotfix

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

Zdroje

https://helpcenter.trendmicro.com/en-us/article/tmka-11252
https://exchange.xforce.ibmcloud.com/vulnerabilities/245173

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

Identifikátor

Apache Shiro - bezpečnostná zraniteľnosť

Popis

Vývojári bezpečnostného frameworku Apache Shiro 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 HTTP požiadavky vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

13.01.2023

CVE

CVE-2023-22602

Zasiahnuté systémy

Apache Shiro vo verzii staršej ako 1.11.0

Následky

Neoprávnená zmena v systéme

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/244693

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

Identifikátor

Panasonic Sanyo CCTV Network Camera - bezpečnostná zraniteľnosť

Popis

Spoločnosť Panasonic vydala bezpečnostnú aktualizáciu na svoj produkt Sanyo CCTV Network Camera, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom CSRF útoku vykonať neoprávnené zmeny v systéme.
Na uvedenú zraniteľnosť je v súčastnosti dostupný proof of concept (POC) kód.

Dátum prvého zverejnenia varovania

12.01.2023

CVE

CVE-2022-4621

Zasiahnuté systémy

Panasonic Sanyo CCTV Network Camera VCC-HD5600P 2.03-06 (všetky verzie)
Panasonic Sanyo CCTV Network Camera VDC-HD3300P 2.03-08 (všetky verzie)
Panasonic Sanyo CCTV Network Camera VDC-HD3300P 1.02-05 (všetky verzie)
Panasonic Sanyo CCTV Network Camera VCC-HD3300 2.03-02 (všetky verzie)
Panasonic Sanyo CCTV Network Camera VDC-HD3100P 2.03-00 (všetky verzie)
Panasonic Sanyo CCTV Network Camera VCC-HD2100P 2.03-02 (všetky verzie)

Následky

Neoprávnené zmeny v systéme

Odporúčania

Nakoľko zasiahnuté systémy už dlhodobo nie sú spoločnosťou Panasonic podporované, používateľom odporúčame prejsť na produkty s aktívnou podporou.
Riadiace systémy a jednotky odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

https://www.cisa.gov/uscert/ics/advisories/icsa-23-012-04

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

Identifikátor

Apache HTTP Server - bezpečnostná zraniteľnosť

Popis

Vývojári webového serveru Apache HTTP Server 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 HTTP požiadavky vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

17.01.2023

CVE

CVE-2022-36760

Zasiahnuté systémy

Apache HTTP Server vo verzii staršej ako 2.4.55

Následky

Neoprávnená zmena v systéme

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://httpd.apache.org/security/vulnerabilities_24.html
https://exchange.xforce.ibmcloud.com/vulnerabilities/244884

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

Identifikátor

Linaro Trusted Firmware-A - bezpečnostná zraniteľnosť

Popis

Vývojári softvéru Trusted Firmware-A vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených X.509 certifikátov získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

16.01.2023

CVE

CVE-2022-47630

Zasiahnuté systémy

Linaro Trusted Firmware-A vo verzii staršej ako f5c51855d36e399e a abb8f936fd0ad085

Následky

Neoprávnený prístup k citlivým údajom

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://trustedfirmware-a.readthedocs.io/en/latest/security_advisories/security-advisory-tfv-10.html
https://exchange.xforce.ibmcloud.com/vulnerabilities/244761
https://seclists.org/oss-sec/2023/q1/30

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

Identifikátor

Dell BIOS - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Dell vydala bezpečnostnú aktualizáciu BIOS na svoje portfólio produktov, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami administrátora prostredníctvom pretečenia zásobníka vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

18.01.2023

CVE

CVE-2022-34393, CVE-2022-34399, CVE-2022-34401, CVE-2022-34460

Zasiahnuté systémy

Dell BIOS vo verzii staršej ako 2022-10-27

Následky

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

Odporúčania

Bezpečnostná záplata je obsiahnutá v aktualizácii UEFI BIOS, preto používateľom odporúčame nainštalovať aktualizácie systému UEFI BIOS z webových stránok výrobcu 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://www.dell.com/support/kbdoc/sk-sk/000204679/dsa-2022-291-dell-client-security-update-for-dell-client-bios
https://www.securitynewspaper.com/2023/01/18/4-critical-bios-vulnerabilities-affect-dell-laptops-like-alienware-inspiron-vostro-models/

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

Identifikátor

Symantec Endpoint Protection - bezpečnostná zraniteľnosť

Popis

Spoločnosť Symantec vydala bezpečnostné aktualizácie na bezpečnostný sofvér Symantec Endpoint Protection, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa eskalovať svoje privilégiá a následne vykonať neoprávnené zmeny v systéme a zneprístupnenie služby.

Dátum prvého zverejnenia varovania

18.01.2023

CVE

CVE-2022-25631

Zasiahnuté systémy

Symantec Endpoint Protection SEP 14.3 vo verzii staršej ako RU6 (14.3.9210.6000)

Následky

Eskalácia privilégií
Neoprávnená zmena v systéme
Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/245137