BEZPEČNOSTNÝ BULLETIN

Týždeň 15. 11. 2023 - 21. 11. 2023

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Intel produkty - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
02.	Chrome a ChromeOS - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
03.	NETGEAR CAX30 - bezpečnostná zraniteľnosť	Vysoká	**8.8**
04.	ManageEngine - bezpečnostná zraniteľnosť	Vysoká	**8.8**
05.	Ashlar-Vellum Lithium - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
06.	Citrix Hypervisor - dve bezpečnostné zraniteľnosti	Vysoká	**8.8**
07.	IBM InfoSphere Information Server - bezpečnostná zraniteľnosť	Vysoká	**8.1**
08.	Splunk Enterprise - bezpečnostná zraniteľnosť	Vysoká	**8.0**
09.	Fortinet produkty - viacero bezpečnostných zraniteľností	Vysoká	**7.8**
10.	Rockwell Automation SIS Workstation a ISaGRAF Workbench	Vysoká	**7.8**
11.	AVEVA produkty - dve bezpečnostné zraniteľnosti	Vysoká	**7.8**
12.	Trend Micro Apex One - viacero bezpečnostných zraniteľností	Vysoká	**7.8**
13.	Avast AVG Antivirus - bezpečnostná zraniteľnosť	Vysoká	**7.8**
14.	MISP - viacero bezpečnostných zraniteľností	Vysoká	**7.5**
15.	TP-Link TL-WR841N - bezpečnostná zraniteľnosť	Vysoká	**7.5**
16.	Dell Precision Tower BIOS - bezpečnostná zraniteľnosť	Vysoká	**7.5**
17.	Cisco produkty - viacero bezpečnostných zraniteľností	Stredná	**6.7**

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-1416

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

Identifikátor

Intel produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Intel vydala bezpečnostné aktualizácie firmvéru 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 prostredníctvom zaslania špeciálne upravených príkazov eskalovať svoje privilégiá a následne získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

14.11.2023

CVE

CVE-2021-46748, CVE-2022-24379, CVE-2022-27229, CVE-2022-28723, CVE-2022-29262, CVE-2022-29510, CVE-2022-33898, CVE-2022-33945, CVE-2022-34301, CVE-2022-34302, CVE-2022-34303, CVE-2022-36374, CVE-2022-36377, CVE-2022-36396, CVE-2022-38786, CVE-2022-41659, CVE-2022-41689, CVE-2022-41700, CVE-2022-42879, CVE-2022-43477, CVE-2022-43666, CVE-2022-45109, CVE-2022-45469, CVE-2022-46298, CVE-2022-46299, CVE-2022-46301, CVE-2022-46646, CVE-2022-46647, CVE-2023-20567, CVE-2023-20568, CVE-2023-22285, CVE-2023-22290, CVE-2023-22292, CVE-2023-22305, CVE-2023-22310, CVE-2023-22313, CVE-2023-22327, CVE-2023-22329, CVE-2023-22337, CVE-2023-22448, CVE-2023-22663, CVE-2023-23583, CVE-2023-24587, CVE-2023-24588, CVE-2023-24592, CVE-2023-25071, CVE-2023-25075, CVE-2023-25080, CVE-2023-25756, CVE-2023-25949, CVE-2023-25952, CVE-2023-26589, CVE-2023-27305, CVE-2023-27306, CVE-2023-27383, CVE-2023-27513, CVE-2023-27519, CVE-2023-27879, CVE-2023-28376, CVE-2023-28377, CVE-2023-28378, CVE-2023-28388, CVE-2023-28397, CVE-2023-28401, CVE-2023-28404, CVE-2023-28723, CVE-2023-28737, CVE-2023-28740, CVE-2023-28741, CVE-2023-29157, CVE-2023-29161, CVE-2023-29165, CVE-2023-29504, CVE-2023-31203, CVE-2023-31273, CVE-2023-32204, CVE-2023-32278, CVE-2023-32279, CVE-2023-32283, CVE-2023-32638, CVE-2023-32641, CVE-2023-32655, CVE-2023-32658, CVE-2023-32660, CVE-2023-32661, CVE-2023-32662, CVE-2023-33872, CVE-2023-33874, CVE-2023-33878, CVE-2023-34314, CVE-2023-34350, CVE-2023-34430, CVE-2023-34431, CVE-2023-34997, CVE-2023-36860, CVE-2023-38131, CVE-2023-38411, CVE-2023-38570, CVE-2023-39221, CVE-2023-39228, CVE-2023-39230, CVE-2023-39411, CVE-2023-39412, CVE-2023-40220, CVE-2023-40540, CVE-2923-22305

Zasiahnuté systémy

2023.4 IPU - BIOS
2023.4 IPU Out-of-Band (OOB) - Intel® Processor
Intel® Arc™ RGB Controller Software
Intel® Battery Life Diagnostic Tool Software
Intel® Chipset Device Software
Intel® Connectivity Performance Suite Software
Intel® Core™ Processors with Radeon™ RX Vega M Graphics
Intel® DCM software
Intel® Ethernet Controllers a Adapters
Intel® FPGA Firmware
Intel® Graphics Drivers
Intel® In-Band Manageability Software
Intel® NUC Firmware
Intel® NUC Software
Intel® OFU Software
Intel® On Demand Agent Software
Intel® oneAPI Toolkit a Component
Intel® OpenVINO™
Intel® Optane™ SSD a Intel® Optane™ SSD DC Firmware
Intel® QAT
Intel® QAT Software
Intel® Rapid Storage Technology Software
Intel® RealSense™ Dynamic Calibration Software
Intel® Server Board a Server System Firmware Advisory
Intel® Server Configuration Utility Software Installer
Intel® Server Information Retrieval Utility Software
Intel® Simics Simulator Software
Intel® Smart Campus Android App
Intel® Support Android App
Intel® Unison™ Software
Intel® XTU Software

Presnú špecifikáciu jednotlivých zasiahnutých produktov nájdete na odkazoch v časti ZDROJE

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.intel.com/content/www/us/en/security-center/advisory/intel-sa-00719.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00758.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00841.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00843.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00861.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00863.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00864.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00869.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00870.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00871.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00894.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00900.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00901.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00902.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00908.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00914.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00924.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00925.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00941.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00943.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00944.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00945.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00950.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00952.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00957.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00961.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00963.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00968.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00971.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00976.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01001.html
https://cloud.google.com/blog/products/identity-security/google-researchers-discover-reptar-a-new-cpu-vulnerability
https://lock.cmpxchg8b.com/reptar.html

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

Identifikátor

Chrome a ChromeOS - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Google vydala bezpečnostné aktualizácie na produkty Chrome a ChromeOS, 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

14.11.2023

CVE

CVE-2023-21216, CVE-2023-35685, CVE-2023-40109, CVE-2023-40110, CVE-2023-40112, CVE-2023-40113, CVE-2023-40114, CVE-2023-40118, CVE-2023-4244, CVE-2023-5197, CVE-2023-5996, CVE-2023-5997, CVE-2023-6112

Zasiahnuté systémy

Chrome pre Mac a Linux vo verzii staršej ako 119.0.6045.159
Chrome pre Windows vo verzii staršej ako 119.0.6045.159/.160
ChromeOS vo verzii staršej ako 15633.44.0

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/2023/11/stable-channel-update-for-desktop_14.html
https://chromereleases.googleblog.com/2023/11/stable-channel-update-for.html

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

Identifikátor

NETGEAR CAX30 - bezpečnostná zraniteľnosť

Popis

Spoločnosť NETGEAR vydala bezpečnostnú aktualizáciu na svoj router CAX30, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje útočníkovi nachádzajúcemu sa v rovnakom sieťovom segmente prostredníctvom zaslania špeciálne vytvorenej požiadavky vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

09.11.2023

CVE

CVE-2023-44445

Zasiahnuté systémy

NETGEAR CAX30 vo verzii firmvéru staršej ako 2.2.1.12

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://kb.netgear.com/000065859/Security-Advisory-for-Pre-authentication-Buffer-Overflow-on-the-CAX30-PSV-2023-0093
https://exchange.xforce.ibmcloud.com/vulnerabilities/271601

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

Identifikátor

ManageEngine - bezpečnostná zraniteľnosť

Popis

Spoločnosť Zoho Corporation vydala bezpečnostnú aktualizáciu na svoj produkt ManageEngine, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených súborov alebo webovej stránky vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

15.11.2023

CVE

CVE-2023-38333

Zasiahnuté systémy

ManageEngine vo verzii staršej ako 16369, 16429, 16519 a 16540

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.manageengine.com/products/applications_manager/security-updates/security-updates-cve-2023-38333.html
https://www.zerodayinitiative.com/advisories/ZDI-23-1715/

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

Identifikátor

Ashlar-Vellum Lithium - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Ashlar-Vellum vydala bezpečnostnú aktualizáciu na svoj produkt Lithium, ktorá opravuje viacero bezpečnostných zraniteľností.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených súborov alebo webovej stránky vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

14.11.2023

CVE

CVE-2023-44437, CVE-2023-44438, CVE-2023-44439, CVE-2023-44440

Zasiahnuté systémy

Ashlar-Vellum Lithium vo verzii staršej ako 12.0.1204.78

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.zerodayinitiative.com/advisories/ZDI-23-1598/
https://www.zerodayinitiative.com/advisories/ZDI-23-1596/
https://www.zerodayinitiative.com/advisories/ZDI-23-1597/
https://www.zerodayinitiative.com/advisories/ZDI-23-1595/

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

Identifikátor

Citrix Hypervisor - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť Citrix vydala bezpečnostnú aktualizáciu na svoj produkt Hypervisor, ktorá opravuje dve bezpečnostné zraniteľnosti.

Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom injekcie špeciálne upravených príkazov eskalovať svoje privilégiá a následne získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

15.11.2023

CVE

CVE-2023-23583, CVE-2023-46835

Zasiahnuté systémy

Citrix Hypervisor 8.2 Cumulative Update 1 vo verzii staršej ako XS82ECU1057

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://support.citrix.com/article/CTX583037/citrix-hypervisor-security-bulletin-for-cve202323583-and-cve202346835
https://exchange.xforce.ibmcloud.com/vulnerabilities/269417
https://exchange.xforce.ibmcloud.com/vulnerabilities/271392

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

Identifikátor

IBM InfoSphere Information Server - bezpečnostná zraniteľnosť

Popis

Spoločnosť IBM vydala bezpečnostnú aktualizáciu na svoj produkt InfoSphere, 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 neoprávnené zmeny v systéme a zneprístupnenie služby.

Dátum prvého zverejnenia varovania

16.11.2023

CVE

CVE-2023-40363

Zasiahnuté systémy

InfoSphere Information Server vo verzii staršej ako 11.7, APAR DT225306

Následky

Neoprávnená zmena v systéme
Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.ibm.com/support/pages/node/7070742
https://exchange.xforce.ibmcloud.com/vulnerabilities/263332

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.0**
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Splunk Enterprise - bezpečnostná zraniteľnosť

Popis

Spoločnosť Splunk vydala bezpečnostnú aktualizáciu na svoj produkt Splunk Enterprise, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zaslania špeciálne vytvoreného XSLT obsahu vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

16.11.2023

CVE

CVE-2023-46214

Zasiahnuté systémy

Splunk Enterprise 9.0 vo verzii staršej ako 9.0.7
Splunk Enterprise 9.1 vo verzii staršej ako 9.1.2
Splunk Cloud vo verzii staršej ako 9.1.2308

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://advisory.splunk.com/advisories/SVD-2023-1104
https://exchange.xforce.ibmcloud.com/vulnerabilities/271693

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

Identifikátor

Fortinet produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Fortinet 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 prostredníctvom podvrhnutia špeciálne vytvorených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

14.11.2023

CVE

CVE-2022-40681, CVE-2023-38545, CVE-2023-38546, CVE-2023-41840

Zasiahnuté systémy

FortiClientWindows 7.2 vo verzii staršej ako 7.2.2
FortiClientWindows 7.0 vo verzii staršej ako 7.0.10
FortiClientWindows 7.2 vo verzii staršej ako 7.2.0
FortiClientWindows 7.0 vo verzii staršej ako 7.0.8
FortiClientWindows 6.4 vo verzii staršej ako 6.4.9
FortiClientWindows vo verzii staršej ako 6.2 (vrátane)
FortiClientWindows vo verzii staršej ako 6.0 (vrátane)
FGT_VM64 vo verzii staršej ako 7.4.2
FGT_VM64 vo verzii staršej ako 7.2.7

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.fortiguard.com/psirt/FG-IR-23-385
https://www.fortiguard.com/psirt/FG-IR-22-299
https://www.fortiguard.com/psirt/FG-IR-23-274
https://exchange.xforce.ibmcloud.com/vulnerabilities/271371

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

Identifikátor

Rockwell Automation SIS Workstation a ISaGRAF Workbench

Popis

Spoločnosť Rockwell Automation vydala bezpečnostné aktualizácie na produkty SIS Workstation a ISaGRAF Workbench, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov 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

14.11.2023

CVE

CVE-2015-9268

Zasiahnuté systémy

Safety Instrumented System Workstation vo verzii staršej ako v2.00
ISaGRAF Workbench vo verzii staršej ako v6.06.10

Následky

Neoprávnená zmena v systéme
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://www.cisa.gov/news-events/ics-advisories/icsa-23-318-02

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

Identifikátor

AVEVA produkty - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť AVEVA vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú 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 úplnú kontrolu nad systémom.

Dátum prvého zverejnenia varovania

14.11.2023

CVE

CVE-2023-33873, CVE-2023-34982

Zasiahnuté systémy

AVEVA Batch Management vo verzii staršej ako 2023
AVEVA Communication Drivers vo verzii staršej ako Pack 2023.1
AVEVA Edge vo verzii staršej ako 2020 R2 SP2
AVEVA Edge vo verzii staršej ako 2023
AVEVA Enterprise Licensing vo verzii staršej ako 4.0
AVEVA MES vo verzii staršej ako 2023
AVEVA Mobile Operator vo verzii staršej ako 2020 R2
AVEVA Operations Control Logger vo verzii staršej ako v22.1 or higher.
AVEVA Plant SCADA vo verzii staršej ako 2023
AVEVA Recipe Management vo verzii staršej ako 2023
AVEVA System Platform vo verzii staršej ako 2020 R2 SP1
AVEVA System Platform vo verzii staršej ako 2023
AVEVA Telemetry Server vo verzii staršej ako 2020 R2 SP2
AVEVA Work Tasks vo verzii staršej ako 2023 SP1
SCADA 2020 vo verzii staršej ako R2 Update 16 (Jun 23)

Následky

Eskalácia privilégií
Zneprístupnenie služby
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.aveva.com/content/dam/aveva/documents/support/cyber-security-updates/SecurityBulletin_AVEVA-2023-003.pdf https://www.cisa.gov/news-events/ics-advisories/icsa-23-318-01

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

Identifikátor

Trend Micro Apex One - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Trend Micro vydala bezpečnostnú aktualizáciu na svoj produkt Apex One, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť sa nachádza vo webovej konzole, spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zaslania špeciálne vytvoreného symbolického odkazu eskalovať svoje privilégiá a následne získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

06.11.2023

CVE

CVE-2023-47192, CVE-2023-47193, CVE-2023-47199, CVE-2023-47200, CVE-2023-47201, CVE-2023-47202

Zasiahnuté systémy

Apex One vo verzii staršej ako SP1 CP 12526
Apex One as a Service vo verzii staršej ako september 2023 (202309), Agent Version 14.0.12737

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://success.trendmicro.com/dcx/s/solution/000295652?language=en_US
https://www.zerodayinitiative.com/advisories/ZDI-23-1621/

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

Identifikátor

Avast AVG Antivirus - bezpečnostná zraniteľnosť

Popis

Spoločnosť Avast vydala bezpečnostnú aktualizáciu na svoj antivírus AVG, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zaslania špeciálne vytvorenej IOCTL 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

15.11.2023

CVE

CVE-2023-5760

Zasiahnuté systémy

AVG Antivirus vo verzii staršej ako 23.9

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/271722

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

Identifikátor

MISP - viacero bezpečnostných zraniteľností

Popis

Vývojári platformy MISP vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

17.11.2023

CVE

CVE-2023-48655, CVE-2023-48656, CVE-2023-48657, CVE-2023-48658, CVE-2023-48659

Zasiahnuté systémy

MISP vo verzii staršej ako v2.4.176

Následky

Neoprávnená zmena v systéme

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.mend.io/vulnerability-database/CVE-2023-48656
https://exchange.xforce.ibmcloud.com/vulnerabilities/271799
https://exchange.xforce.ibmcloud.com/vulnerabilities/271798
https://exchange.xforce.ibmcloud.com/vulnerabilities/271797
https://exchange.xforce.ibmcloud.com/vulnerabilities/271794
https://exchange.xforce.ibmcloud.com/vulnerabilities/271800
https://github.com/MISP/MISP/commit/d6ad402b31547c95280a6d8320f8f87a8f609074

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

Identifikátor

TP-Link TL-WR841N - bezpečnostná zraniteľnosť

Popis

Spoločnosť TP-Link vydala bezpečnostnú aktualizáciu na svoj router TL-WR841N, ktorá opravuje bezpečnostnú zraniteľnosť.
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 s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

14.11.2023

CVE

CVE-2023-39471

Zasiahnuté systémy

TL-WR841N s firmvérom vo verzii staršej ako v14_US_0.9.1_4.19

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/271570
https://www.zerodayinitiative.com/advisories/ZDI-23-1624/

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

Identifikátor

Dell Precision Tower BIOS - bezpečnostná zraniteľnosť

Popis

Spoločnosť Dell vydala bezpečnostné aktualizácie na produkty Precision Tower 5820, 7820 a 7920, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami administrátora prostredníctvom zaslania špeciálne vytvorenej požiadavky vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

15.11.2023

CVE

CVE-2023-32469

Zasiahnuté systémy

Dell Precision 5820 Tower vo verzii staršej ako 2.32.0
Dell Precision 7820 Tower vo verzii staršej ako 2.36.0
Dell Precision 7920 Tower vo verzii staršej ako 2.36.0

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://www.dell.com/support/kbdoc/en-us/000216242/dsa-2023-223-security-update-for-a-dell-precision-tower-bios-vulnerability
https://exchange.xforce.ibmcloud.com/vulnerabilities/271730

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 6.7
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 Cisco Identity Services Engine a spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami administrátora prostredníctvom zaslania špeciálne vytvorených súborov získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

15.11.2023

CVE

CVE-2023-20084, CVE-2023-20208, CVE-2023-20240, CVE-2023-20241, CVE-2023-20265, CVE-2023-20272, CVE-2023-20274

Zasiahnuté systémy

IP DECT 110 Single-Cell Base Station with Multiplatform Firmware (CSCwf58578)
IP DECT 210 Multi-Cell Base Station with Multiplatform Firmware (CSCwf58578)
Unified IP Phone 6901 (CSCwf58592)
Unified SIP Phone 3905 (CSCwf58594)
Secure Client AnyConnect for Android
Secure Client AnyConnect VPN for iOS
Secure Client (including AnyConnect) for Universal Windows Platform
Secure Client for Linux
Secure Client for MacOS
Cisco AppDynamics PHP Agent
Cisco ISE
Cisco Secure Endpoint Connector for Windows
Cisco Secure Endpoint Private Cloud

Presnú špecifikáciu jednotlivých zasiahnutých produktov nájdete na odkazoch v časti ZDROJE

Následky

Úplné narušenie dôvernosti, integrity a dostupnosti systému
Zneprístupnenie služby
Eskalácia privilégií

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-1416

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-accsc-dos-9SLzkZ8 https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-uipphone-xss-NcmUykqA https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-appd-php-authpriv-gEBwTvu5 https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-mult-j-KxpNynR https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-secure-endpoint-dos-RzOgFKnd

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-1416