BEZPEČNOSTNÝ BULLETIN

Týždeň 11. 01. 2023 - 17. 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-996

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

Identifikátor

Microsoft produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Microsoft vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť sa nachádza v produkte Microsoft SharePoint Server, spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

10.01.2023

CVE

CVE-2023-21524, CVE-2023-21525, CVE-2023-21531, CVE-2023-21532, CVE-2023-21535, CVE-2023-21536, CVE-2023-21537, CVE-2023-21539, CVE-2023-21540, CVE-2023-21541, CVE-2023-21542, CVE-2023-21543, CVE-2023-21546, CVE-2023-21548, CVE-2023-21549, CVE-2023-21550, CVE-2023-21551, CVE-2023-21552, CVE-2023-21555, CVE-2023-21556, CVE-2023-21557, CVE-2023-21558, CVE-2023-21559, CVE-2023-21560, CVE-2023-21561, CVE-2023-21563, CVE-2023-21674, CVE-2023-21675, CVE-2023-21676, CVE-2023-21678, CVE-2023-21679, CVE-2023-21680, CVE-2023-21681, CVE-2023-21682, CVE-2023-21724, CVE-2023-21725, CVE-2023-21726, CVE-2023-21730, CVE-2023-21732, CVE-2023-21733, CVE-2023-21734, CVE-2023-21735, CVE-2023-21736, CVE-2023-21737, CVE-2023-21738, CVE-2023-21739, CVE-2023-21741, CVE-2023-21742, CVE-2023-21744, CVE-2023-21745, CVE-2023-21746, CVE-2023-21747, CVE-2023-21748, CVE-2023-21749, CVE-2023-21750, CVE-2023-21752, CVE-2023-21753, CVE-2023-21754, CVE-2023-21755, CVE-2023-21759, CVE-2023-21760, CVE-2023-21761, CVE-2023-21762, CVE-2023-21763, CVE-2023-21764, CVE-2023-21765, CVE-2023-21766, CVE-2023-21767, CVE-2023-21768, CVE-2023-21771, CVE-2023-21772, CVE-2023-21773, CVE-2023-21774, CVE-2023-21776, CVE-2023-21779, CVE-2023-21780, CVE-2023-21781, CVE-2023-21782, CVE-2023-21783, CVE-2023-21784, CVE-2023-21785, CVE-2023-21786, CVE-2023-21787, CVE-2023-21788, CVE-2023-21789, CVE-2023-21790, CVE-2023-21791, CVE-2023-21792, CVE-2023-21793

Zasiahnuté systémy

.NET Core
3D Builder
Azure Service Fabric Container
Microsoft Bluetooth Driver
Microsoft Edge (Chromium-based)
Microsoft Exchange Server
Microsoft Graphics Component
Microsoft Local Security Authority Server (lsasrv)
Microsoft Message Queuing
Microsoft Office
Microsoft Office SharePoint
Microsoft Office Visio
Microsoft WDAC OLE DB provider for SQL

Visual Studio Code
Windows ALPC
Windows Ancillary Function Driver for WinSock
Windows Authentication Methods
Windows Backup Engine
Windows Bind Filter Driver
Windows BitLocker
Windows Boot Manager
Windows Credential Manager
Windows Cryptographic Services
Windows DWM Core Library
Windows Error Reporting
Windows Event Tracing
Windows IKE Extension
Windows Installer
Windows Internet Key Exchange (IKE) Protocol
Windows iSCSI
Windows Kernel
Windows Layer 2 Tunneling Protocol
Windows LDAP - Lightweight Directory Access Protocol
Windows Local Security Authority (LSA)
Windows Local Session Manager (LSM)
Windows Malicious Software Removal Tool
Windows Management Instrumentation
Windows MSCryptDImportKey
Windows NTLM
Windows ODBC Driver
Windows Overlay Filter
Windows Point-to-Point Tunneling Protocol
Windows Print Spooler Components
Windows Remote Access Service L2TP Driver
Windows RPC API
Windows Secure Socket Tunneling Protocol (SSTP)
Windows Smart Card
Windows Task Scheduler
Windows Virtual Registry Provider
Windows Workstation Service

Presnú špecifikáciu zasiahnutých produktov nájdete na odkaze v časti ZDROJE.

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje
https://msrc.microsoft.com/update-guide/releaseNote/2023-Jan

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

Identifikátor

Google Chrome - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Google vydala bezpečnostnú aktualizáciu na svoj internetový prehliadač Chrome, ktorá opravuje 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

10.01.2023

CVE

CVE-2023-0128, CVE-2023-0129, CVE-2023-0130, CVE-2023-0131, CVE-2023-0132, CVE-2023-0133, CVE-2023-0134, CVE-2023-0135, CVE-2023-0136, CVE-2023-0137, CVE-2023-0138, CVE-2023-0139, CVE-2023-0140, CVE-2023-0141

Zasiahnuté systémy

Chrome vo verzii staršej ako 109.0.5414.74 (linux)
Chrome vo verzii staršej ako 109.0.5414.74/.75(Windows)
Chrome vo verzii staršej ako 109.0.5414.87(Mac)

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.
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://chromereleases.googleblog.com/2023/01/stable-channel-update-for-desktop.html
https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-google-chrome-could-allow-for-arbitrary-code-execution_2023-005

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

Identifikátor

Zoom - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Zoom Video Communications 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 eskalovať svoje privilégiá a následne získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

06.01.2023

CVE

CVE-2022-36925, CVE-2022-36926, CVE-2022-36927, CVE-2022-36928, CVE-2022-36929, CVE-2022-36930

Zasiahnuté systémy

Zoom Rooms pre Windows vo verzii staršej ako 5.13.0
Zoom Rooms pre macOS vo verzii staršej ako 5.11.4
Zoom pre Android vo verzii staršej ako 5.13.0

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://explore.zoom.us/en/trust/security/security-bulletin/

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

Identifikátor

NVIDIA Omniverse Kit - bezpečnostná zraniteľnosť

Popis

Spoločnosť NVIDIA vydala bezpečnostné aktualizácie na produkty z balíka Omniverse Kit, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

10.01.2023

CVE

CVE-2022-42268

Zasiahnuté systémy

Omniverse Audio2Face vo verzii staršej ako 2022.2
Omniverse Create vo verzii staršej ako 2022.3
NVIDIA Isaac Sim vo verzii staršej ako 2022.2.0
Omniverse Machinima vo verzii staršej ako 2022.3
Omniverse Code vo verzii staršej ako 2022.3.0
Omniverse View vo verzii staršej ako 2022.2.1

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov a aplikovať odporúčania výrobcu, ktoré môžete nájsť na odkaze v časti ZDROJE.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.
Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://nvidia.custhelp.com/app/answers/detail/a_id/5418

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

Identifikátor

Zyxel CPE, ONT, WIFI extenders - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Zyxel vydala bezpečnostné aktualizácie na svoje portfólio routerov, optických sieťových terminálov a wi-fi extendérov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej požiadavky vykonať škodlivý kód alebo neprístupnenie služby.

Dátum prvého zverejnenia varovania

11.01.2023

CVE

CVE-2022-43389, CVE-2022-43390, CVE-2022-43391, CVE-2022-43392

Zasiahnuté systémy

Zyxel 5G NR/4G LTE CPE
Zyxel Fiber ONT
Zyxel DSL/Ethernet CPE
Zyxel WiFi extender
Presnú špecifikáciu jednotlivých zasiahnutých produktov nájdete na odkazoch v časti ZDROJE

Následky

Vykonanie škodlivého kódu
Zneprístupnenie služby

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.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-command-injection-and-buffer-overflow-vulnerabilities-of-cpe-fiber-onts-and-wifi-extenders
https://exchange.xforce.ibmcloud.com/vulnerabilities/244382

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

Identifikátor

JATOS - bezpečnostná zraniteľnosť

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnosti softvéru pre hostovanie online experimentov JATOS.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvoreného súboru vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

06.01.2023

CVE

CVE-2022-4878

Zasiahnuté systémy

JATOS vo verzii staršej ako 3.7.5 (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.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.
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/244127

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

Identifikátor

Adobe produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Adobe vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšie bezpečnostné zraniteľnosti spočívajú v nedostatočnej implementácii bezpečnostných mechanizmov a umožňujú lokálnemu, neautentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

10.01.2023

CVE

CVE-2023-21579, CVE-2023-21581, CVE-2023-21585, CVE-2023-21586, CVE-2023-21587, CVE-2023-21588, CVE-2023-21589, CVE-2023-21590, CVE-2023-21591, CVE-2023-21592, CVE-2023-21604, CVE-2023-21605, CVE-2023-21606, CVE-2023-21607, CVE-2023-21608, CVE-2023-21609, CVE-2023-21610, CVE-2023-21611, CVE-2023-21612, CVE-2023-21613, CVE-2023-21614

Zasiahnuté systémy

Acrobat DC vo verzii staršej ako 22.003.20310
Acrobat Reader DC vo verzii staršej ako 22.003.20310
Acrobat 2020 vo verzii staršej ako 20.005.30436
Acrobat Reader 2020 vo verzii staršej ako 20.005.30436
Adobe InDesign vo verzii staršej ako ID18.1
Adobe InDesign vo verzii staršej ako ID17.4.1
Adobe InCopy vo verzii staršej ako ID17.4.1
Adobe InCopy vo verzii staršej ako ID18.1
Adobe Dimension vo verzii staršej ako 3.4.7

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.

Zdroje
https://helpx.adobe.com/security/products/acrobat/apsb23-01.html https://helpx.adobe.com/security/products/indesign/apsb23-07.html https://helpx.adobe.com/security/products/incopy/apsb23-08.html https://helpx.adobe.com/security/products/dimension/apsb23-10.html https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-adobe-products-could-allow-for-arbitrary-code-execution_2023-004

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

Identifikátor

Intel oneAPI Toolkit - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Intel vydala bezpečnostné aktualizácie na produkty oneAPI DPC++/C++ Compiler a C++ Compiler Classic, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa zneužitím bližšie nešpecifikovanej zraniteľnosti eskalovať svoje privilégiá a následne získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť znepristupnenie služby.

Dátum prvého zverejnenia varovania

10.01.2023

CVE

CVE-2022-38136, CVE-2022-40196, CVE-2022-41342

Zasiahnuté systémy

Intel® oneAPI DPC++/C++ Compiler vo verzii staršej ako 2022.2.1.
Intel® C++ Compiler Classic vo verzii staršej ako 2021.8.

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-00773.html

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.7**
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

AMD EPYC CPU - viacero bezpečnostných zraniteľností

Popis

Spoločnosť AMD vydala bezpečnostné aktualizácie na svoje portfólio procesorov EPYC, ktoré opravujú viacero bezpečnostných zraniteľností v AMD Secure Processor (ASP), AMD System Management Unit (SMU) a AMD Secure Encrypted Virtualization (SEV).
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej požiadavky vykonať neoprávnené zmeny v systéme a zneprístupnenie služby.

Dátum prvého zverejnenia varovania

10.01.2023

CVE

CVE-2021-26316, CVE-2021-26328, CVE-2021-26343, CVE-2021-26353, CVE-2021-26355, CVE-2021-26396, CVE-2021-26398, CVE-2021-26402, CVE-2021-26403, CVE-2021-26404, CVE-2021-26407, CVE-2021-26409, CVE-2021-39298, CVE-2021-46767, CVE-2021-46768, CVE-2021-46779, CVE-2021-46791, CVE-2022-23813, CVE-2022-23814, CVE-2023-20522, CVE-2023-20523, CVE-2023-20525, CVE-2023-20527, CVE-2023-20528, CVE-2023-20529, CVE-2023-20530, CVE-2023-20531, CVE-2023-20532

Zasiahnuté systémy

AMD EPYC procesory 1., 2. a 3. generácie
Presnú špecifikáciu jednotlivých zasiahnutých produktov nájdete na odkaze v sekcii ZDROJE

Následky

Vykonanie škodlivého kódu
Zneprístupnenie služby
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 zariadenie.

Zdroje

https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-1032
https://exchange.xforce.ibmcloud.com/vulnerabilities/244402

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

Identifikátor

Black Box KVM - bezpečnostná zraniteľnosť

Popis

Spoločnosť Black Box vydala bezpečnostnú aktualizáciu na switche rady KVM, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej HTTP požiadavky získať neoprávnený prístup k citlivým údajom.
Na uvedenú zraniteľnosť je dostupný Proof-of-Concept kód.

Dátum prvého zverejnenia varovania

10.01.2023

CVE

CVE-2022-4636

Zasiahnuté systémy

Black Box KVM ACR1000A-R-R2 vo verzii firmvéru staršej ako 3.6
Black Box KVM ACR1000A-T-R2 vo verzii firmvéru staršej ako 3.6
Black Box KVM ACR1002A-T vo verzii firmvéru staršej ako 3.6
Black Box KVM ACR1002A-R vo verzii firmvéru staršej ako 3.6
Black Box KVM ACR1020A-T vo verzii firmvéru staršej ako 3.6

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.
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-23-010-01