BEZPEČNOSTNÝ BULLETIN

Týždeň 15. 02. 2023 - 21. 02. 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-1044

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.8**
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.
Najzávažnejšia 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

14.02.2023

CVE

CVE-2023-21574, CVE-2023-21575, CVE-2023-21576, CVE-2023-21577, CVE-2023-21578, CVE-2023-21583, CVE-2023-21584, CVE-2023-21593, CVE-2023-21619, CVE-2023-21620, CVE-2023-21621, CVE-2023-21622, CVE-2023-22226, CVE-2023-22227, CVE-2023-22228, CVE-2023-22229, CVE-2023-22230, CVE-2023-22231, CVE-2023-22232, CVE-2023-22233, CVE-2023-22234, CVE-2023-22236, CVE-2023-22237, CVE-2023-22238, CVE-2023-22239, CVE-2023-22243, CVE-2023-22244, CVE-2023-22246

Zasiahnuté systémy

Adobe Substance 3D Stager
Adobe Animate
Adobe Premiere Rush
Adobe InDesign
Adobe Photoshop
Adobe Bridge
Adobe FrameMaker
Adobe Connect
Adobe After Effects

Presnú špecifikáciu jednotlivých zasiahnutých produktov nájdete na odkazoch v sekcii 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.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.

Zdroje
https://www.cybersecurity-help.cz/vdb/SB2023021564
https://helpx.adobe.com/security/products/after_effects/apsb23-02.html
https://helpx.adobe.com/security/products/substance3d_stager/apsb23-16.html
https://helpx.adobe.com/security/products/animate/apsb23-15.html
https://helpx.adobe.com/security/products/indesign/apsb23-12.html
https://helpx.adobe.com/security/products/photoshop/apsb23-11.html
https://helpx.adobe.com/security/products/bridge/apsb23-09.html
https://helpx.adobe.com/security/products/framemaker/apsb23-06.html
https://helpx.adobe.com/security/products/connect/apsb23-05.html

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

15.02.2023

CVE

CVE-2023-0616, CVE-2023-0767, CVE-2023-25728, CVE-2023-25729, CVE-2023-25730, CVE-2023-25731, CVE-2023-25732, CVE-2023-25733, CVE-2023-25734, CVE-2023-25735, CVE-2023-25736, CVE-2023-25737, CVE-2023-25738, CVE-2023-25739, CVE-2023-25740, CVE-2023-25741, CVE-2023-25742, CVE-2023-25743, CVE-2023-25744, CVE-2023-25745, CVE-2023-25746

Zasiahnuté systémy

Thunderbird vo verzii staršej ako 102.8
Firefox ESR vo verzii staršej ako 102.8
Firefox vo verzii staršej ako 110

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/mfsa2023-05/
https://www.mozilla.org/en-US/security/advisories/mfsa2023-06/

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

Identifikátor

SAP produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť SAP vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť sa nachádza v SAP Host Agent Service, spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zaslania špeciálne vytvorenej požiadavky získať úplnú kontrolu nad systémom.

Dátum prvého zverejnenia varovania

14.02.2023

CVE

CVE-2022-41262, CVE-2022-41264, CVE-2022-41268, CVE-2023-0013, CVE-2023-0019, CVE-2023-0020, CVE-2023-0024, CVE-2023-0025, CVE-2023-23851, CVE-2023-23852, CVE-2023-23853, CVE-2023-23854, CVE-2023-23855, CVE-2023-23856, CVE-2023-23858, CVE-2023-23859, CVE-2023-23860, CVE-2023-24521, CVE-2023-24522, CVE-2023-24523, CVE-2023-24524, CVE-2023-24525, CVE-2023-24528, CVE-2023-24529, CVE-2023-24530, CVE-2023-25614

Zasiahnuté systémy

SAP Business Client
SAP Host Agent Service
SAP BASIS
SAP BusinessObjects Business Intelligence platform
SAP Business Planning and Consolidation
SAP Solution Manager
SAP Solution Manager (BSP Application)
SAP GRC Process Control application
SAP Fiori
SAP S/4 HANA
SAP NetWeaver

Presnú špecifikáciu jednotlivých zasiahnutých produktov nájdete na odkaze v sekcii ZDROJE

Následky

Vykonanie škodlivého kódu
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.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html https://nvd.nist.gov/vuln/detail/CVE-2023-24523

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

Identifikátor

Schneider Electric produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Schneider Electric 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 vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

14.02.2023

CVE

CVE-2011-4859, CVE-2018-7240, CVE-2018-7241, CVE-2018-7242, CVE-2020-28895, CVE-2020-35198, CVE-2020-35683, CVE-2020-35684, CVE-2020-35685, CVE-2020-7562, CVE-2020-7563, CVE-2020-7564, CVE-2021-22785, CVE-2021-22787, CVE-2021-22788, CVE-2021-31400, CVE-2021-31401, CVE-2022-0222, CVE-2022-43376, CVE-2022-43377, CVE-2022-43378, CVE-2023-0595, CVE-2023-25547, CVE-2023-25548, CVE-2023-25549, CVE-2023-25550, CVE-2023-25551, CVE-2023-25552, CVE-2023-25553, CVE-2023-25554, CVE-2023-25555, CVE-2023-25556

Zasiahnuté systémy

EcoStruxure TM Geo SCADA Expert 2019 vo verziách starších ako Október 2022
EcoStruxure TM Geo SCADA Expert 2020 vo verziách starších ako Október 2022
EcoStruxure TM Geo SCADA Expert 2021 vo verziách starších ako Október 2022
ClearSCADA vo všetkých verziách
StruxureWare Data Center Expert V7.9.2 and earlier
Merten INSTABUS Tastermodul 1fach System M 625199 Program vo verzii 1.0
Merten INSTABUS Tastermodul 2fach System M 625299 Program vo verzii 1.0
Merten Tasterschnittstelle 4fach plus 670804 Program vo verzii 1.0 & Program vo verzii 1.2
Merten KNX ARGUS 180/2,20M UP SYSTEM 631725 Program vo verzii 1.0
Merten Jalousie-/Schaltaktor REG-K/8x/16x/10 m. HB 649908 (Product discontinued) Program vo verzii 1.0
Merten KNX Uni-Dimmaktor LL REG-K/2x230/300 W MEG6710-0002 (Product discontinued) Program vo verzii 1.0 & Program vo verzii 1.1
Merten KNX Schaltakt.2x6A UP m.2 Eing. MEG6003-0002 (Product discontinued) Program vo verzii 0.1
NetBotz 4 - 355/450/455/550/570vo verzii staršej ako V4.7.0 (vrátane)
Modicon M340 CPUs BMXP34* vo verzii staršej ako V3.40
Modicon Ethernet BMXNOE0100 (H) vo verzii staršej ako SV03.50
Modicon Ethernet BMXNOE0110 (H) vo verzii staršej ako SV06.70
Modicon Ethernet BMXNOR* vo verzii staršej ako v1.7 IR24
Modicon Ethernet Communication Module BMXNOE0100 (H) vo verzii staršej ako SV03.50
Modicon Ethernet Communication Module BMXNOE0110 (H) vo verzii staršej ako SV06.70
Modicon Ethernet Communication Module BMXNOC0401 vo verzii staršej ako V2.11
Modicon Ethernet Communication Module BMXNOR0200H RTU vo verzii staršej ako V1.7 IR24

Modicon Premium processor with integrated Ethernet COPRO TSXP574634 vo všetkých verziách
Modicon Premium processor with integrated Ethernet COPRO TSXP575634 vo všetkých verziách
Modicon Premium processor with integrated Ethernet COPRO TSXP576634 vo všetkých verziách
Modicon Quantum processor with integrated Ethernet COPRO 140CPU65xxxxx vo všetkých verziách
Modicon Quantum communication Module 140NOE771x1 vo všetkých verziách
Modicon Quantum communication Module 140NOC78x00 vo všetkých verziách
Modicon Quantum communication Module 140NOC77101 vo všetkých verziách
Modicon Premium communication Module TSXETY4103 vo všetkých verziách
Modicon Premium communication Module TSXETY5103 vo všetkých verziách
Lexium ILE ILA ILS communication drive Firmware communication module vo verzii staršej ako V01.111
Altivar 32/320/340/600/900 Profinet communication module (VW3A3627) Firmware vo verzii staršej ako V1.10.1
Altivar 32/320 and Lexium 32 Ethernet TCP/IP communication module (VW3A3616) vo všetkých verziách
Altivar 61/71 Profinet communication card (VW3A3327) vo všetkých verziách
M340 CPUs M340 P34x vo verzii staršej ako V3.40
Modicon Ethernet Communication Module BMXNOR0200H vo verzii staršej ako V1.7 IR 23
Premium Processors with Integrated Ethernet COPRO TSXP574634, TSXP575634, TSXP576634 vo všetkých verziách
Premium Communication Module 140CPU65xxxxx, vo všetkých verziách
Quantum Communication Module 140NOE771x1 vo všetkých verziách
Quantum Communication Module 140NOC78x00 vo všetkých verziách
Quantum Communication Module 140NOC77101 vo všetkých verziách
Modicon M340, V3.50
Modicon M340 vo verziách starších ako V3.40 (vrátane)
Modicon M580 vo verziách starších ako V3.20 (vrátane)
Modicon M580 CPU Safety
Modicon RTU:BMXNOR0200H, vo verzii staršej ako V1.7 IR24
Modicon M340 Ethernet Communication Module BMXNOE0100 (H), vo verzii SV03.50
Modicon M340 Ethernet Communication Module BMXNOE0110 (H), vo verzii SV06.70
Modicon X80 Ethernet Communication Module BMXNOC0401, vo verzii staršej ako V2.11
Legacy Modicon Premium and Quantum, vo všetkých verziách

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

Zdroje
https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2018-081-01&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2018-081-01_Embedded_FTP_Servers_for_Modicon_PAC_Controllers_Security_Notification.pdf&_ga=2.157909370.1747170292.1676964438-1407605564.1661159793
https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2020-315-01&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2020-315-01_Modicon_Web_Server_Security_Notification.pdf&_ga=2.157909370.1747170292.1676964438-1407605564.1661159793
https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-257-02&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2021-257-02_Web_Server_Modicon_M340_Quantum_and_Premium_and_Communication_Modules.pdf&_ga=2.157909370.1747170292.1676964438-1407605564.1661159793
https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-313-05&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2021-313-05_BadAlloc_Vulnerabilities_Security_Notification.pdf&_ga=2.157909370.1747170292.1676964438-1407605564.1661159793+
https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2022-102-02&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2022-102-02_Modicon_M340_Controller_and_Communication_ModuleSecurity_Notification.pdf&_ga=2.157909370.1747170292.1676964438-1407605564.1661159793
https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2022-312-01&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2022-312-01-NetBotz_4_Security_Notification.pdf&_ga=2.157909370.1747170292.1676964438-1407605564.1661159793
https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-045-03&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-045-03.pdf&_ga=2.157909370.1747170292.1676964438-1407605564.1661159793
https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-045-02&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-045-02.pdf&_ga=2.157909370.1747170292.1676964438-1407605564.1661159793
https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-045-01&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-045-01.pdf&_ga=2.157909370.1747170292.1676964438-1407605564.1661159793

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

Identifikátor

B&R produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť B&R 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 administrátora eskalovať svoje privilégiá a následne získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

15.02.2023

CVE

CVE-2020-27339, CVE-2020-5953, CVE-2021-33625, CVE-2021-33626, CVE-2021-33627, CVE-2021-41837, CVE-2021-41838, CVE-2021-41839, CVE-2021-41841, CVE-2021-42059, CVE-2021-42060, CVE-2021-42113, CVE-2021-42554, CVE-2021-43323, CVE-2021-43522, CVE-2021-43615, CVE-2021-45969, CVE-2021-45970, CVE-2021-45971, CVE-2022-24030, CVE-2022-24031, CVE-2022-24069

Zasiahnuté systémy

APC 3100 vo verzii staršej ako 1.40
APC 2200 vo verzii staršej ako 1.30
PPC 3100 vo verzii staršej ako 1.40
PPC 2200 vo verzii staršej ako 1.30
PPC 1200 vo verzii staršej ako 1.10
PPC 80 vo verzii staršej ako 1.10
MPC 3100 vo verzii staršej ako 1.20

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.

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.br-automation.com/downloads_br_productcatalogue/assets/1675931547567-en-original-1.0.pdf

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

Identifikátor

Splunk Enterprise - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Splunk vydala bezpečnostnú aktualizáciu na svoj produkt Splunk Enterprise, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup k citlivým údajom a vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

15.02.2023

CVE

CVE-2021-28957, CVE-2021-3517, CVE-2021-3518, CVE-2021-3537, CVE-2022-24785, CVE-2022-31129, CVE-2022-32212, CVE-2022-42889, CVE-2023-22932, CVE-2023-22933, CVE-2023-22934, CVE-2023-22935, CVE-2023-22939

Zasiahnuté systémy

Splunk Enterprise vo verziách starších ako 8.1.13, 8.2.10, a 9.0.4

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.
Ak používateľ nevyužíva komponent Splunk Web, výrobca ho odporúča deaktivovať.

Zdroje

https://advisory.splunk.com/advisories
https://nvd.nist.gov/vuln/detail/CVE-2023-22939
https://www.securityweek.com/splunk-enterprise-updates-patch-high-severity-vulnerabilities/

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

Identifikátor

AMD Ryzen™ Master - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť AMD vydala bezpečnostnú aktualizáciu pre svoj firmvér Ryzen™ Master, ktorá opravuje dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom podvrhnutia špeciálne vytvorených súborov eskalovať svoje privilégiá a následne vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

15.02.2023

CVE

CVE-2022-27672, CVE-2022-27677

Zasiahnuté systémy

Ryzen™ Master vo verzii staršej ako 2.10.1.2287

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://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1045
https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1052

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

Identifikátor

Citrix - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Citrix 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 úplnú kontrolu nad systémom.

Dátum prvého zverejnenia varovania

16.02.2023

CVE

CVE-2023-24483, CVE-2023-24484, CVE-2023-24485, CVE-2023-24486

Zasiahnuté systémy

Citrix Virtual Apps and Desktops vo verzii staršej ako 2212
Citrix Virtual Apps and Desktops 2203 LTSR vo verzii staršej ako CU2
Citrix Virtual Apps and Desktops 1912 LTSR vo verzii staršej ako CU6
Citrix Workspace App for Windows vo verzii staršej ako 2212
Citrix Workspace App for Windows 2203 LTSR vo verzii staršej ako CU2
Citrix Workspace App for Windows 1912 LTSR vo verzii staršej ako CU6
Citrix Workspace App for Linux vo verzii staršej ako 2302

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.securityweek.com/citrix-patches-high-severity-vulnerabilities-in-windows-linux-apps/
https://support.citrix.com/article/CTX477618/citrix-workspace-app-for-linux-security-bulletin-for-cve202324486
https://support.citrix.com/article/CTX477617/citrix-workspace-app-for-windows-security-bulletin-for-cve202324484-cve202324485
https://support.citrix.com/article/CTX477616/citrix-virtual-apps-and-desktops-security-bulletin-for-cve202324483

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

Identifikátor

Zyxel produkty - tri bezpečnostné zraniteľnosti

Popis

Spoločnosť Zyxel vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú tri bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť nachádzajúca sa vo firewalloch rady ATP, USG FLEX, VPN, ZyWALL/USG spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami administrátora prostredníctvom injekcie špeciálne upravených príkazov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

07.02.2023

CVE

CVE-2022-38547, CVE-2022-45441, CVE-2022-45854

Zasiahnuté systémy

NWA110AX vo verzii staršej ako 6.50(ABTG.0)C0
NWA210AX vo verzii staršej ako 6.50(ABTD.0)C0
WAX510D vo verzii staršej ako 6.50(ABTF.0)C0
WAX610D vo verzii staršej ako 6.50(ABTE.0)C0
WAX630S vo verzii staršej ako 6.50(ABZD.0)C0
WAX650S vo verzii staršej ako 6.50(ABRM.0)C0
ATP vo verzii staršej ako ZLD V5.35
USG FLEX vo verzii staršej ako ZLD V5.35
VPN vo verzii staršej ako ZLD V5.35
ZyWALL/USG vo verzii staršej ako ZLD V4.73
NBG-418N v2 vo verzii staršej ako V1.00(AARP.13)C0

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému
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.
Administrátorom odporúčame limitovať prístup k administratívnemu rozhraniu a jeho funkciám zavedením zoznamu pre riadenie prístupov (ACL).

Zdroje
https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-xss-vulnerability-in-nbg-418n-v2-home-router https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-post-authentication-rce-in-firewalls https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-dos-vulnerability-of-aps

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

Identifikátor

GoAnywhere MFT - bezpečnostná zraniteľnosť

Popis

Spoločnosť Fortra vydala bezpečnostnú aktualizáciu na svoj softvér pre prenos súborov GoAnywhere MFT, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami administrátora prostredníctvom injekcie špeciálne upravených príkazov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

06.02.2023

CVE

CVE-2023-0669

Zasiahnuté systémy

GoAnywhere MFT vo verzii staršej ako 7.1.2.

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://nvd.nist.gov/vuln/detail/CVE-2023-0669
https://www.darkreading.com/endpoint/massive-goanywhere-rce-exploit
https://www.goanywhere.com/services/upgrades