BEZPEČNOSTNÝ BULLETIN

Týždeň 06. 12. 2023 - 12. 12. 2023

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	CODESYS Control produkty - bezpečnostná zraniteľnosť	Vysoká	**8.8**
02.	SolarWinds Orion Platform - bezpečnostná zraniteľnosť	Vysoká	**8.8**
03.	Tenda smerovače - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
04.	Apple produkty - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
05.	Brocade Fabric OS - bezpečnostná zraniteľnosť	Vysoká	**8.1**
06.	QNAP produkty - viacero bezpečnostných zraniteľností	Vysoká	**8.0**
07.	IEC61850 Server (Telecontrol) - bezpečnostná zraniteľnosť	Vysoká	**7.5**
08.	Dell PowerScale OneFS a OS10 Networking Switches - tri bezpečnostné zraniteľnosti	Vysoká	**7.5**
09.	ControlByWeb X-332 a X-301 - bezpečnostná zraniteľnosť	Vysoká	**7.5**
10.	Johnson Controls Metasys a Facility Explorer - bezpečnostná zraniteľnosť	Vysoká	**7.5**
11.	SonicWall SMA100 SSL-VPN - dve bezpečnostné zraniteľnosti	Vysoká	**7.2**
12.	HP-UX System Management Homepage - bezpečnostná zraniteľnosť	Vysoká	**7.2**
13.	Mattermost Server - bezpečnostná zraniteľnosť	Vysoká	**7.1**
14.	ZTC Industrial ZT410 a ZTC Desktop GK420d - bezpečnostná zraniteľnosť	Stredná	**5.4**
15.	Schweitzer Engineering Laboratories SEL-411L - bezpečnostná zraniteľnosť	Stredná	**4.3**
16.	Counter-Strike 2 - bezpečnostná zraniteľnosť	Stredná	**4.3**

Národný bezpečnostný úrad
Budatínska 30
851 06 Bratislava

Mail: sk-cert@nbu.gov.sk
Mobil: +421 903 993 706
Tel: +421 2 6869 2915

SK-CERT
Naša značka:
01794/2022/SK-CERT-1441

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

Identifikátor

CODESYS Control produkty - bezpečnostná zraniteľnosť

Popis

Spoločnosť CODESYS vydala bezpečnostné aktualizácie na svoje portfólio produktov CODESYS Control, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom injekcie špeciálne upravených príkazov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

05.12.2023

CVE

CVE-2023-6357

Zasiahnuté systémy

CODESYS Control for BeagleBone SL vo verzii staršej ako 4.11.0.0
CODESYS Control for emPC-A/iMX6 SL vo verzii staršej ako 4.11.0.0
CODESYS Control for IOT2000 SL vo verzii staršej ako 4.11.0.0
CODESYS Control for Linux ARM SL vo verzii staršej ako 4.11.0.0
CODESYS Control for Linux SL vo verzii staršej ako 4.11.0.0
CODESYS Control for PFC100 SL vo verzii staršej ako 4.11.0.0
CODESYS Control for PFC200 SL vo verzii staršej ako 4.11.0.0
CODESYS Control for PLCnext SL vo verzii staršej ako 4.11.0.0
CODESYS Control for Raspberry Pi SL vo verzii staršej ako 4.11.0.0
CODESYS Control for WAGO Touch Panels 600 SL vo verzii staršej ako 4.11.0.0
CODESYS Runtime Toolkit for Linux or QNX vo verzii staršej ako 3.5.19.50

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu. Ak je potrebný vzdialený prístup, použite virtuálnu súkromnú sieť (VPN). Administrátorom odporúčame filtrovať sieťovú komunikáciu bezpečnostnými prvkami sieťovej infraštruktúry.

Zdroje

https://cert.vde.com/en/advisories/VDE-2023-066/

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

Identifikátor

SolarWinds Orion Platform - bezpečnostná zraniteľnosť

Popis

Spoločnosť SolarWinds vydala bezpečnostnú aktualizáciu na svoj produkt Orion Platform, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom SQL injekcie vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

05.12.2023

CVE

CVE-2023-40056

Zasiahnuté systémy

SolarWinds Platform vo verzii staršej ako 2023.4.2

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://documentation.solarwinds.com/en/success_center/orionplatform/content/release_notes/solarwinds_platform_2023-4-2_release_notes.htm

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

Identifikátor

Tenda smerovače - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Tenda vydala bezpečnostné aktualizácie na routre W30E, AX12 a AX9, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť zasahuje router W30E, spočíva v nedostatočnom overovaní používateľských vstupov 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

08.12.2023

CVE

CVE-2023-49402, CVE-2023-49403, CVE-2023-49404, CVE-2023-49405, CVE-2023-49406, CVE-2023-49408, CVE-2023-49409, CVE-2023-49410, CVE-2023-49411, CVE-2023-49424, CVE-2023-49425, CVE-2023-49426, CVE-2023-49428, CVE-2023-49429, CVE-2023-49430, CVE-2023-49431, CVE-2023-49432, CVE-2023-49433, CVE-2023-49434, CVE-2023-49435, CVE-2023-49436, CVE-2023-49437, CVE-2023-49999, CVE-2023-50000, CVE-2023-50001, CVE-2023-50002

Zasiahnuté systémy

Tenda W30E vo verzii firmvéru staršej ako V16.01.0.12 (4843)
Tenda AX12 vo verzii firmvéru staršej ako V22.03.01.46
Tenda AX9 vo verzii firmvéru staršej ako V22.03.01.46

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/273478
https://github.com/GD008/TENDA/blob/main/w30e/tenda_w30e_setUmountUSBPartition/w30e_setUmountUSBPartition.md
https://github.com/GD008/TENDA/blob/main/w30e/tenda_w30e_resetMesh/w30e_resetMesh.md
https://github.com/GD008/TENDA/blob/main/w30e/tenda_w30e_upgradeMeshOnline/w30e_upgradeMeshOnline.md
https://github.com/GD008/TENDA/blob/main/w30e/tenda_w30e_rebootMesh/w30e_rebootMesh.md
https://github.com/GD008/TENDA/blob/main/w30e/tenda_w30e_deleteMesh/w30e_deleteMesh.md
https://github.com/ef4tless/vuln/blob/master/iot/AX12/SetVirtualServerCfg.md
https://github.com/ef4tless/vuln/blob/master/iot/AX12/setMacFilterCfg.md
https://github.com/ef4tless/vuln/blob/master/iot/AX12/SetStaticRouteCfg.md
https://github.com/ef4tless/vuln/blob/master/iot/AX12/SetOnlineDevName.md
https://github.com/ef4tless/vuln/blob/master/iot/AX12/SetNetControlList-3.md
https://github.com/ef4tless/vuln/blob/master/iot/AX9/setDeviceInfo.md
https://github.com/ef4tless/vuln/blob/master/iot/AX9/SetStaticRouteCfg.md
https://github.com/ef4tless/vuln/blob/master/iot/AX9/SetOnlineDevName.md
https://github.com/ef4tless/vuln/blob/master/iot/AX9/setMacFilterCfg.md
https://github.com/ef4tless/vuln/blob/master/iot/AX9/SetVirtualServerCfg.md
https://github.com/ef4tless/vuln/blob/master/iot/AX9/SetNetControlList-2.md
https://github.com/ef4tless/vuln/blob/master/iot/AX9/SetNetControlList-3.md
https://github.com/ef4tless/vuln/blob/master/iot/AX9/SetNetControlList-2.md

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

Identifikátor

Apple produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Apple 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.
Zraniteľnosti sú v súčasnosti aktívne zneužívané útočníkmi.

Dátum prvého zverejnenia varovania

11.12.2023

CVE

CVE-2020-19185, CVE-2020-19186, CVE-2020-19187, CVE-2020-19188, CVE-2020-19189, CVE-2020-19190, CVE-2023-42842, CVE-2023-42874, CVE-2023-42882, CVE-2023-42883, CVE-2023-42884, CVE-2023-42886, CVE-2023-42890, CVE-2023-42891, CVE-2023-42894, CVE-2023-42897, CVE-2023-42898, CVE-2023-42899, CVE-2023-42900, CVE-2023-42901, CVE-2023-42902, CVE-2023-42903, CVE-2023-42904, CVE-2023-42905, CVE-2023-42906, CVE-2023-42907, CVE-2023-42908, CVE-2023-42909, CVE-2023-42910, CVE-2023-42911, CVE-2023-42912, CVE-2023-42914, CVE-2023-42916, CVE-2023-42917, CVE-2023-42919, CVE-2023-42922, CVE-2023-42923, CVE-2023-42924, CVE-2023-42926, CVE-2023-42927, CVE-2023-42932, CVE-2023-45866, CVE-2023-5344

Zasiahnuté systémy

iOS vo verzii staršej ako 17.2
iPadOS vo verzii staršej ako 17.2
iOS vo verzii staršej ako 16.7.3
iPadOS vo verzii staršej ako 16.7.3
macOS Sonoma vo verzii staršej ako 14.2
macOS Ventura vo verzii staršej ako 13.6.3
macOS Monterey vo verzii staršej ako 12.7.2
tvOS vo verzii staršej ako 17.2
watchOS vo verzii staršej ako 10.2
Safari vo verzii staršej ako 17.2

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

Zdroje
https://support.apple.com/en-us/HT214039 https://support.apple.com/en-us/HT214041 https://support.apple.com/en-us/HT214040 https://support.apple.com/en-us/HT214037 https://support.apple.com/en-us/HT214038 https://support.apple.com/en-us/HT214036 https://support.apple.com/en-us/HT214034 https://support.apple.com/en-us/HT214035

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

Identifikátor

Brocade Fabric OS - bezpečnostná zraniteľnosť

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnosti produktu Brocade Fabric OS.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej požiadavky podvrhnúť, autentifikovať a aktivovať licenčný kľúč, a tak získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

06.12.2023

CVE

CVE-2021-27795

Zasiahnuté systémy

Brocade X6-8 director prevádzkujúci akúkoľvek verziu FOS below v9.1.1
Brocade X6-8 director (switch type 166.0) prevádzkujúci verziu FOS v9.1.1 alebo vyššiu
Brocade X6-4 director prevádzkujúci akúkoľvek verziu FOS nižšiu ako v9.1.1
Brocade X6-4 director (switch type 165.0) prevádzkujúci verziu FOS v9.1.1 alebo vyššiu
Brocade G630 switche (switch type 173) prevádzkujúce akúkoľvek verziu FOS
Brocade G620 switche (switch type 162) prevádzkujúce akúkoľvek verziu FOS
Brocade G610 switche (switch types 170.0, 170.1, 170.2) prevádzkujúce akúkoľvek verziu FOS
Brocade 6520 switche prevádzkujúce akúkoľvek verziu FOS
Brocade 6510 switche prevádzkujúce akúkoľvek verziu FOS
Brocade 6505 switche prevádzkujúce akúkoľvek verziu FOS
Brocade 7840 extension switche prevádzkujúce akúkoľvek verziu FOS
Brocade 7810 extension switche prevádzkujúce akúkoľvek verziu FOS
Brocade 7800 extension switche prevádzkujúce akúkoľvek verziu FOS
Brocade 300 switche prevádzkujúce akúkoľvek verziu FOS
Všetky Embedded Brocade switche prevádzkujúce akúkoľvek verziu FOS

Následky

Eskalácia privilégií
Neoprávnený prísup k citlivým údajom
Neoprávnená zmena v systéme
Zneprístupnenie služby

Odporúčania
Administrátorom a používateľom odporúčame postupovať podľa pokynov výrobcu, ktoré môžete nájsť na odkazoch v časti ZDROJE. 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.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/21289 https://nvd.nist.gov/vuln/detail/CVE-2021-27795

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

Identifikátor

QNAP produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť QNAP vydala bezpečnostnú aktualizáciu na svoje portfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť sa nachádza vo firmvéri QNAP VioStor NVR, spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje autentifikovanému útočníkovi s právomocami používateľa, ktorý sa nachádza 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

09.12.2023

CVE

CVE-2023-23372, CVE-2023-32968, CVE-2023-32975, CVE-2023-3961, CVE-2023-4091, CVE-2023-4154, CVE-2023-42669, CVE-2023-42670, CVE-2023-47565

Zasiahnuté systémy

QTS 5.0.x vo verzii staršej ako QTS 5.0.1.2514 build 20230906
QTS 5.1.x vo verzii staršej ako QTS 5.1.3.2578 build 20231110
QuTS hero h5.0.x vo verzii staršej ako QuTS hero h5.0.1.2515 build 20230907
QuTS hero h5.1.x vo verzii staršej ako QuTS hero h5.1.3.2578 build 20231110
QVR Firmware 4.x vo verzii staršej ako QVR Firmware 5.x

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.qnap.com/uploads/security-advisories/QSA-23-48/CVE-2023-47565.json
https://www.qnap.com/en/security-advisory/qsa-23-20
https://www.qnap.com/en/security-advisory/qsa-23-40
https://www.qnap.com/en/security-advisory/qsa-23-48
https://www.qnap.com/en/security-advisory/qsa-23-07

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

Identifikátor

IEC61850 Server (Telecontrol) - bezpečnostná zraniteľnosť

Popis

Spoločnosť Wago vydala bezpečnostnú aktualizáciu na svoju knižnicu WagoAppRTU používanú v rámci produktu WAGO Telecontrol Configurator, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne upravených paketov spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

05.12.2023

CVE

CVE-2023-5188

Zasiahnuté systémy

WagoAppRTU vo verzii staršej ako 1.4.6.0

Následky

Zneprístupnenie služby

Odporúčania

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

Zdroje

https://cert.vde.com/en/advisories/VDE-2023-044/

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

Identifikátor

Dell PowerScale OneFS a OS10 Networking Switches - tri bezpečnostné zraniteľnosti

Popis

Spoločnosť Dell vydala bezpečnostné aktualizácie na produkty PowerScale OneFS a OS10 Networking Switches, ktoré opravujú tri bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť sa nachádza v produktoch OS10 Networking Switches, spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi spôsobiť zneprístupnenie služby. Zraniteľnosť je možné zneužiť na switchoch konfigurovaných s VLT a VRRP.
Zraniteľnosti v produkte PowerScale OneFS by útočník mohol zneužiť na neoprávnený prístup k citlivým údajom alebo zneprístupnenie služby.

Dátum prvého zverejnenia varovania

05.12.2023

CVE

CVE-2023-39248, CVE-2023-44288, CVE-2023-44295

Zasiahnuté systémy

PowerScale OneFS vo verzii staršej ako 9.4.0.16
Dell Networking vo verzii staršej ako OS10 10.5.5.6

Následky

Neoprávnený prístup k citlivým údajom
Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.dell.com/support/kbdoc/en-us/000219932/dsa-2023-417-dell-powerscale-onefs-security-updates-for-multiple-security-vulnerabilities
https://www.dell.com/support/kbdoc/en-us/000220138/dsa-2023-278-dell-networking-os10-security-updates-for-uncontrolled-resource-consumption

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

Identifikátor

ControlByWeb X-332 a X-301 - bezpečnostná zraniteľnosť

Popis

Spoločnosť ControlByWeb vydala bezpečnostné aktualizácie na produkty X-332 a X-301, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami administrátora vykonať vykonať škodlivý JavaScript kód (stored XSS).

Dátum prvého zverejnenia varovania

07.12.2023

CVE

CVE-2023-6333

Zasiahnuté systémy

X301 vo verzii firmvéru staršej ako V1.20
X332 vo verzii firmvéru staršej ako V1.09

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.cisa.gov/news-events/ics-advisories/icsa-23-341-05

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

Identifikátor

Johnson Controls Metasys a Facility Explorer - bezpečnostná zraniteľnosť

Popis

Spoločnosť Johnson Controls vydala bezpečnostné aktualizácie na svoje portfólio produktov Metasys a Facility Explorer, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania neplatných prihlasovacích údajov spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

07.12.2023

CVE

CVE-2023-4486

Zasiahnuté systémy

Metasys NAE55 engines vo verzii staršej ako 12.0.4
Metasys SNE engines vo verzii staršej ako 12.0.4
Metasys SNC engines vo verzii staršej ako 12.0.4
Facility Explorer F4-SNC engine vo verzii staršej ako 11.0.6
Facility Explorer F4-SNC engine vo verzii staršej ako 12.0.4

Následky

Zneprístupnenie služby

Odporúčania

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

Zdroje

https://www.johnsoncontrols.com/cyber-solutions/security-advisories
https://www.cisa.gov/news-events/ics-advisories/icsa-23-341-03

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

Identifikátor

SonicWall SMA100 SSL-VPN - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť SonicWall vydala bezpečnostnú aktualizáciu na svoj produkt SMA100 SSL-VPN, ktorá opravuje dve bezpečnostné zraniteľnosti.
Najzávažnejšia zraniteľnosť s označením CVE-2023-44221 spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, 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

04.12.2023

CVE

CVE-2023-44221, CVE-2023-5970

Zasiahnuté systémy

SMA 100 Series(SMA 200, 210, 400, 410, 500v) vo verzii staršej ako 10.2.1.10-62sv

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://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0018

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

Identifikátor

HP-UX System Management Homepage - bezpečnostná zraniteľnosť

Popis

Spoločnosť Hewlett Packard enterprise vydala bezpečnostnú aktualizáciu na svoj produkt HP-UX System Management Homepage, ktorá opravuje bezpečnostnú zraniteľnosť.
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

08.12.2023

CVE

CVE-2023-50271

Zasiahnuté systémy

HP-UX System Management Homepage vo verzii staršej ako A.3.2.23.09

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť získanie prístupu k citlivým údajom je dobrou praxou zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbux04551en_us

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

Identifikátor

Mattermost Server - bezpečnostná zraniteľnosť

Popis

Vývojári platformy Mattermost Server vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zaslania špeciálne vytvorenej požiadavky vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

05.12.2023

CVE

CVE-2023-6458

Zasiahnuté systémy

Mattermost Server vo verzii staršej ako 9.1.2
Mattermost Server v6 vo verzii staršej ako 7.8.14
Mattermost Server v8 vo verzii staršej ako 8.1.5, 9.0.3

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://github.com/advisories/GHSA-7664-hcp7-f497
https://mattermost.com/security-updates/

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 5.4
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

ZTC Industrial ZT410 a ZTC Desktop GK420d - bezpečnostná zraniteľnosť

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnosti tlačiarní od spoločnosti Zebra Technologies.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii mechanizmov autentifikácie a umožňuje útočníkovi nachádzajúcemu sa v rovnakom sieťovom segmente prostredníctvom zaslania špeciálne vytvorenej požiadavky získať neoprávnený prístup k citlivým údajom a vykonať neoprávnené zmeny v systéme.
Zraniteľnosť je možné zneužiť len na tlačiarňach s deaktivovaným režimom "Protected Mode".

Dátum prvého zverejnenia varovania

05.12.2023

CVE

CVE-2023-4957

Zasiahnuté systémy

ZTC Industrial ZT410
ZTC Desktop GK420d

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov a tlačiarne prevádzkovať výlučne v režime "Protected Mode".
Po odstránení zraniteľností, ktoré mohli spôsobiť získanie prístupu k citlivým údajom je dobrou praxou zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://www.cisa.gov/news-events/ics-advisories/icsa-23-339-01

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 4.3
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Schweitzer Engineering Laboratories SEL-411L - bezpečnostná zraniteľnosť

Popis

Spoločnosť Schweitzer Engineering vydala bezpečnostné aktualizácie na svoje portfólio produktov SEL-411L, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi zrealizovať tzv. clickjacking útoky.

Dátum prvého zverejnenia varovania

07.12.2023

CVE

CVE-2023-2265

Zasiahnuté systémy

SEL-411L R118 vo verzii V0 až V3 (vrátane)
SEL-411L R119 vo verzii V0 až V4 (vrátane)
SEL-411L R120 vo verzii V0 až V5 (vrátane)
SEL-411L R121 vo verzii V0 až V2 (vrátane)
SEL-411L R122 vo verzii V0 až V2 (vrátane)
SEL-411L R123 vo verzii V0 až V2 (vrátane)
SEL-411L R124 vo verzii V0 až V2 (vrátane)
SEL-411L R125 vo verzii V0 až V2 (vrátane)
SEL-411L R126 vo verzii V0 až V3 (vrátane)
SEL-411L R127 vo verzii V0 až V1 (vrátane)
SEL-411L R128 vo verzii V0 (vrátane)
SEL-411L R129 vo verzii V0 (vrátane)

Následky

Vykonanie škodlivého kódu

Odporúčania

Spoločnosť Schweitzer Engineering už distribuovala záplaty vlastníkom zasiahnutých zariadení.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu. Ak je potrebný vzdialený prístup, použite virtuálnu súkromnú sieť (VPN). Administrátorom odporúčame filtrovať sieťovú komunikáciu bezpečnostnými prvkami sieťovej infraštruktúry.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.

Zdroje

https://www.cisa.gov/news-events/ics-advisories/icsa-23-341-02
https://selinc.com/support/security-notifications/external-reports/

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 4.3
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Counter-Strike 2 - bezpečnostná zraniteľnosť

Popis

Spoločnosť Valve vydala bezpečnostnú aktualizáciu na svoju počítačovú hru Counter-Strike 2, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom injekcie škodlivého skriptu získať IP adresy svojich spoluhráčov.

Dátum prvého zverejnenia varovania

11.12.2023

CVE

-

Zasiahnuté systémy

Counter-Strike 2 vo verzii staršej ako Build 12931567 (11.12.2023)

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.bleepingcomputer.com/news/security/counter-strike-2-html-injection-bug-exposes-players-ip-addresses/