BEZPEČNOSTNÝ BULLETIN

Týždeň 06. 10. 2021 - 12. 10. 2021

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:
01439/2020/SK-CERT-580

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

Identifikátor

Cisco Small Business 220 switches - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Cisco vydala bezpečnostnú aktualizáciu na svoje produkty Small Business 220 switches, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje neautentifikovanému útočníkovi, ktorý sa nachádza v rovnakom sieťovom segmente prostredníctvom zasielania špeciálne upravených paketov, vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

06.10.2021

CVE

CVE-2021-34775, CVE-2021-34776, CVE-2021-34777, CVE-2021-34778, CVE-2021-34779, CVE-2021-34780

Zasiahnuté systémy

Cisco Small Business 220 Series Smart Switches s firmware vo verzii staršej ako 1.2.1.2

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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T
https://www.securityweek.com/cisco-patches-high-severity-vulnerabilities-security-appliances-business-switches

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

Identifikátor

Dahua kamery - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť Dahua vydala bezpečnostnú aktualizáciu na svoje portfólio produktov, ktoré opravujú dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii mechanizmov autentifikácie a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne upravených paketov, vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.
Na uvedenú zraniteľnosť je v súčasnosti voľne dostupný Proof-of-Concept kód.

Dátum prvého zverejnenia varovania

07.10.2021

CVE

CVE-2021-33044, CVE-2021-33045

Zasiahnuté systémy

DH_IPC-HX3XXX-Leo_MultiLang_PN_Stream3 vo verzii staršej ako V2.800.0000000.29.R.210630
DH_IPC-HX3XXX-Leo_MultiLang_NP_Stream3 vo verzii staršej ako V2.800.0000000.29.R.210630
DH_IPC-HX3XXX-Dalton_MultiLang_NP_Stream3 vo verzii staršej ako V2.820.0000000.18.R.210705
DH_IPC-HX3XXX-Dalton_MultiLang_PN_Stream3 vo verzii staršej ako V2.820.0000000.18.R.210705
DH_IPC-HX5XXX-Volt_MultiLang_PN_Stream3 vo verzii staršej ako V2.820.0000000.5.R.210705
DH_IPC-HX5XXX-Volt_MultiLang_NP_Stream3 vo verzii staršej ako V2.820.0000000.5.R.210705
DH_IPC-HUM7XXX-E2-Volt_MultiLang_NP vo verzii staršej ako V2.820.0000000.5.R.210705
DH_IPC-HUM7XXX-E2-Volt_MultiLang_PN vo verzii staršej ako V2.820.0000000.5.R.210705
DH_VTO75X95X_Eng_PN_SIP vo verzii staršej ako V4.300.0000003.0.R.210714
DH_VTO65XXX_Eng_PN vo verzii staršej ako V4.300.0000004.0.R.210715
DH_VTH542XH_MultiLang_SIP vo verzii staršej ako V4.500.0000002.0.R.210715
DH_SD-Eos-Civil_MultiLang_PN_Stream3 vo verzii staršej ako V2.812.0000007.0.R.210706
DH_SD-Eos-Civil_MultiLang_NP_Stream3 vo verzii staršej ako V2.812.0000007.0.R.210706
DH_SD-Eos_MultiLang_PN_Stream3 vo verzii staršej ako V2.812.0000007.0.R.21070
DH_SD-Eos_MultiLang_NP_Stream3 vo verzii staršej ako V2.812.0000007.0.R.210706
DH_TPC-BF1241-TB_MultiLang_PN vo verzii staršej ako V2.630.0000000.6.R.210707
DH_TPC-BF1241-TB_MultiLang_NP vo verzii staršej ako V2.630.0000000.6.R.210707
DH_TPC-BF2221-TB_MultiLang_PN vo verzii staršej ako V2.630.0000000.10.R.210707
DH_TPC-BF2221-TB_MultiLang_NP vo verzii staršej ako V2.630.0000000.10.R.210707
DH_TPC-SD2221-TB_MultiLang_PN vo verzii staršej ako V2.630.0000000.7.R.210707
DH_TPC-SD2221-TB_MultiLang_NP vo verzii staršej ako V2.630.0000000.7.R.210707
DH_TPC-BF5X01-TB_MultiLang_PN vo verzii staršej ako V2.630.0000000.12.R.210707
DH_TPC-BF5X01-TB_MultiLang_NP vo verzii staršej ako V2.630.0000000.12.R.210707
DH_TPC-BF5X21-TB_MultiLang_PN vo verzii staršej ako V2.630.0000000.8.R.210630
DH_TPC-BF5X21-TB_MultiLang_NP vo verzii staršej ako V2.630.0000000.8.R.210630

DH_TPC-PT8X21A-TB_MultiLang_PN vo verzii staršej ako V2.630.0000000.14.R.210630
DH_TPC-PT8X21A-TB_MultiLang_NP vo verzii staršej ako V2.630.0000000.14.R.210630
DH_TPC-SD8X21-TB_MultiLang_PN vo verzii staršej ako V2.630.0000000.9.R.210706
DH_TPC-SD8X21-TB_MultiLang_NP vo verzii staršej ako V2.630.0000000.9.R.210706
DH_TPC-PT8X21B-B_MultiLang_PN vo verzii staršej ako V2.630.0000000.10.R.210701
DH_TPC-PT8X21B-B_MultiLang_NP vo verzii staršej ako V2.630.0000000.10.R.210701
DH_NVR4XXX-I_MultiLang vo verzii staršej ako V4.001.0000000.3.R.210710
DH_NVR4x-4KS2L_MultiLang vo verzii staršej ako V4.001.0000001.0.R.210709
DH_NVR4XXX-4KS2_MultiLang vo verzii staršej ako V4.001.0000005.1.R.210713
DH_NVR5XXX-4KS2_MultiLang vo verzii staršej ako V4.001.0000006.1.R.210709
DH_NVR5XXX-I_MultiLang vo verzii staršej ako V4.001.0000000.3.R.210710
DH_NVR5XXX-IL_MultiLang vo verzii staršej ako V4.001.0000000.0.R.210710
DH_NVR1XHC-S3_MultiLang vo verzii staršej ako V4.001.0000000.1.R.210710
DH_NVR2XXX-4KS2_MultiLang vo verzii staršej ako V4.001.0000005.0.R.210709
DH_NVR2XXX-W-4KS2_MultiLang vo verzii staršej ako V4.001.0000003.1.R.210709
DH_NVR2XXX-I2_Mul vo verzii staršej ako V4.002.0000000.0.R.210709
DH_NVR2XXX-I_Mul vo verzii staršej ako V4.001.0000000.1.R.210710
DH_NVR1XXX-S3H_MultiLang vo verzii staršej ako V4.001.0000005.1.R.210709
DH_NVR6XX-4KS2_MultiLang vo verzii staršej ako V4.001.0000001.1.R.210716
DH_XVR5x16-I2_MultiLang vo verzii staršej ako V4.001.0000003.1.R.210710
DH_XVR7x16-I2_MultiLang vo verzii staršej ako V4.001.0000003.1.R.210710
DH_XVR5x08-I2_MultiLang vo verzii staršej ako V4.001.0000003.1.R.210710
DH_XVR5x04-I2_MultiLang vo verzii staršej ako V4.001.0000003.1.R.210710
DH_XVR7x32-I2_MultiLang vo verzii staršej ako V4.001.0000003.1.R.210710
DH_XVR5x08-I3_MultiLang vo verzii staršej ako V4.001.0000000.15.R.210702
DH_XVR5x04-I3_MultiLang vo verzii staršej ako V4.001.0000000.15.R.210702
DH_XVR4x08-I3_MultiLang vo verzii staršej ako V4.001.0000000.15.R.210702
DH_XVR4x04-I_MultiLang vo verzii staršej ako V4.001.0000001.1.R.210709
DH_XVR4x08-I_MultiLang vo verzii staršej ako V4.001.0000001.1.R.210709
DH_XVR5x08-X_MultiLang vo verzii staršej ako V4.001.0000000.9.R.210710
DH_XVR5x16-X_MultiLang vo verzii staršej ako V4.001.0000000.9.R.210710
DH_XVR7x16-X_MultiLang vo verzii staršej ako V4.001.0000000.9.R.210710
DH_XVR5x04-X1(2.0)_MultiLang vo verzii staršej ako V4.001.0000000.14.R.210709
DH_XVR4x04-X1(2.0)_MultiLang vo verzii staršej ako V4.001.0000000.14.R.210709

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.

Zdroje
https://www.dahuasecurity.com/support/cybersecurity/details/957 https://www.bleepingcomputer.com/news/security/unpatched-dahua-cams-vulnerable-to-unauthenticated-remote-access/ https://github.com/mcw0/DahuaConsole

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

Identifikátor

Emerson WirelessHART Gateway produkt - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Emerson vydala bezpečnostnú aktualizáciu na produkt WirelessHART Gateway, ktorá opravuje 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

05.10.2021

CVE

CVE-2021-03554, CVE-2021-10073, CVE-2021-22439, CVE-2021-24769, CVE-2021-81019, CVE-2021-85337

Zasiahnuté systémy

WirelessHART 1410 Gateway vo verzii staršej ako v4.7.105
WirelessHART 1410D Gateway vo verzii staršej ako v4.7.105
WirelessHART 1420 Gateway vo verzii staršej ako v4.7.105

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.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

https://us-cert.cisa.gov/ics/advisories/icsa-21-278-02

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

Identifikátor

FATEK Automation WinProladder - viacero bezpečnostných zraniteľností

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnostiach produktu WinProladder od spoločnosti FATEK.

Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov 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

07.10.2021

CVE

CVE-2021-38426, CVE-2021-38430, CVE-2021-38434, CVE-2021-38436, CVE-2021-38438, CVE-2021-38440, CVE-2021-38442

Zasiahnuté systémy

WinProladder vo verzii staršej ako 3.30 (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.

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.

Administrátorom odporúčame limitovať prístup k administratívnemu rozhraniu a jeho funkciám zavedením zoznamu pre riadenie prístupov (ACL).

Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

https://us-cert.cisa.gov/ics/advisories/icsa-21-280-06

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

Identifikátor

Yamale balík pre Python - bezpečnostná zraniteľnosť

Popis

Vývojári balíka Yamale vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov 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

07.10.2021

CVE

CVE-2021-38305

Zasiahnuté systémy

Yamale vo verzii staršej ako 3.0.8

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Odporúčame uistiť sa, či Vaše aplikácie nevyužívajú frameworky, knižnice, pluginy, SDK alebo moduly v zraniteľnej verzii. V prípade, že áno, zabezpečte aktualizáciu všetkých komponentov, od ktorých závisí vaša aplikácia, na aktuálne verzie bez známych bezpečnostných zraniteľností.
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://github.com/23andMe/Yamale/releases/tag/3.0.8
https://thehackernews.com/2021/10/code-execution-bug-affects-yamale.html
https://nvd.nist.gov/vuln/detail/CVE-2021-38305

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

Identifikátor

Exacq Technologies exacqVision Server - bezpečnostná zraniteľnosť

Popis

Spoločnosť Exacq Technologies vydala bezpečnostnú aktualizáciu na produkt exacqVision Server, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

07.10.2021

CVE

CVE-2021-27665

Zasiahnuté systémy

exacqVision Server 32-bit vo verzii staršej ako 21.09

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

https://us-cert.cisa.gov/ics/advisories/icsa-21-280-03
https://www.johnsoncontrols.com/cyber-solutions/security-advisories

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

Identifikátor

Mitsubishi Electric GOT a Tension Controller - viacero bezpečnostných zraniteľností

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnostiach produktov GOT a Tension Controller od spoločnosti Mitsubishi Electric.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne vytvorených paketov, spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

05.10.2021

CVE

CVE-2021-20602, CVE-2021-20603, CVE-2021-20604, CVE-2021-20605

Zasiahnuté systémy

GT2107-WTBD všetky verzie
GT2107-WTSD všetky verzie
GT2104-RTBD všetky verzie
GT2104-PMBD všetky verzie
GT2103-PMBD všetky verzie
GS2110-WTBD všetky verzie
GS2107-WTBD všetky verzie
GS2110-WTBD-N všetky verzie
GS2107-WTBD-N všetky verzie
LE7-40GU-L všetky verzie

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame sledovať stránku výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu zasiahnutých systémov.
Výrobca odporúča zapnúť filtrovanie IP adries podľa postupu uvedeného na webovej adrese:
https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-014_en.pdf
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-014_en.pdf
https://us-cert.cisa.gov/ics/advisories/icsa-21-278-01