BEZPEČNOSTNÝ BULLETIN

Týždeň 09. 10. 2019 - 15. 10. 2019

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Microsoft produkty viacero zraniteľností	Vysoká	**8.8**
02.	Intel produkty viacero zraniteľností	Vysoká	**8.8**
03.	NitroPDF viacero zraniteľností	Vysoká	**8.8**
04.	Google Chrome viacero zraniteľností	Vysoká	**8.8**
05.	Modicon zraniteľnosti	Vysoká	**8.6**
06.	Siemens produkty viacero zraniteľností	Vysoká	**7.9**
07.	Phoenix Contact Automationworx Suite zraniteľnosť	Vysoká	**7.8**
08.	Linux Sudo zraniteľnosť	Vysoká	**7.8**
09.	Dell ImageAssist zraniteľnosť	Vysoká	**7.5**
10.	Zraniteľnosť tlačiarní Samsung	Vysoká	**7.5**

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:
01380/2019/SK-CERT-248

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

Identifikátor

Microsoft produkty viacero zraniteľností

Popis

Spoločnosť Microsoft vydala bezpečnostné aktualizácie na svoje produkty, ktoré opravujú 59 bezpečnostných zraniteľností.
Najzávažnejšie zraniteľnosti v komponente VBScript umožňujú vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených súborov vykonať škodlivý kód a spôsobiť úplné narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

08.10.2019

CVE

CVE-2019-0608, CVE-2019-1060, CVE-2019-1070, CVE-2019-1166, CVE-2019-1230, CVE-2019-1238,
CVE-2019-1239, CVE-2019-1307, CVE-2019-1308, CVE-2019-1311, CVE-2019-1313, CVE-2019-1314,
CVE-2019-1315, CVE-2019-1316, CVE-2019-1317, CVE-2019-1318, CVE-2019-1319, CVE-2019-1320,
CVE-2019-1321, CVE-2019-1322, CVE-2019-1323, CVE-2019-1325, CVE-2019-1326, CVE-2019-1327,
CVE-2019-1328, CVE-2019-1329, CVE-2019-1330, CVE-2019-1331, CVE-2019-1333, CVE-2019-1334,
CVE-2019-1335, CVE-2019-1336, CVE-2019-1337, CVE-2019-1338, CVE-2019-1339, CVE-2019-1340,
CVE-2019-1341, CVE-2019-1342, CVE-2019-1343, CVE-2019-1344, CVE-2019-1345, CVE-2019-1346,
CVE-2019-1347, CVE-2019-1356, CVE-2019-1357, CVE-2019-1358, CVE-2019-1359, CVE-2019-1361,
CVE-2019-1362, CVE-2019-1363, CVE-2019-1364, CVE-2019-1365, CVE-2019-1366, CVE-2019-1368,
CVE-2019-1369, CVE-2019-1371, CVE-2019-1372, CVE-2019-1375, CVE-2019-1376, CVE-2019-1378

Zasiahnuté systémy

Microsoft Windows
Internet Explorer
Microsoft Edge (EdgeHTML-based)
ChakraCore
Microsoft Office and Microsoft Office Services and Web Apps
SQL Server Management Studio
Microsoft Dynamics 365
Windows Update Assistant
Azure App Service

Následky

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

Odporúčania

Administrátorom odporúčame bezodkladne 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://thehackernews.com/2019/10/microsoft-patch-tuesday-october.html https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/28ef0a64-489c-e911-a994-000d3a33c573 https://exchange.xforce.ibmcloud.com/vulnerabilities/168422 https://www.bleepingcomputer.com/news/microsoft/microsofts-october-2019-patch-tuesday-fixes-59-vulnerabilities/

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

Identifikátor

Intel produkty viacero zraniteľností

Popis

Spoločnosť Intel vydala bezpečnostné aktualizácie na svoje produkty, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšie zraniteľnosti vo firmvéri Intel NUC umožňujú lokálnemu, autentifikovanému útočníkovi eskalovať svoje privilégiá.

Dátum prvého zverejnenia varovania

08.10.2019

CVE

CVE-2019-11120, CVE-2019-11167, CVE-2019-14569, CVE-2019-14570

Zasiahnuté systémy

Intel® Active System Console for Intel® Server Boards a systémy založené na Intel® 62X Chipset verzie staršie ako 8.0 Build 24.
Intel® Smart Connect Technology for Intel® NUC
Intel® NUC 8 Mainstream Game Kit verzie staršie ako INWHL357
Intel® NUC 8 Mainstream Game Mini Computer verzie staršie ako INWHL357
Intel® NUC Board DE3815TYBE (H26998-500 & later) verzie staršie ako TY0022
Intel® NUC Kit DE3815TYKHE (H27002-500 & later) verzie staršie ako TY0022
Intel® NUC Board DE3815TYBE verzie staršie ako TY0067
Intel® NUC Kit DE3815TYKHE verzie staršie ako TY0067
Intel® NUC Kit DN2820FYKH verzie staršie ako FY0069

Následky

Eskalácia privilégií
Zneprístupnenie služby
Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré môžu spôsobiť únik informácií, 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-00261.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00286.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00296.html

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

Identifikátor

NitroPDF viacero zraniteľností

Popis

Bezpečnostní výskumníci informovali o viacerých zraniteľnostiach v produkte NitroPDF.
Najzávažnejšie bezpečnostné zraniteľnosti sú spôsobené nesprávnym spracovaním používateľských vstupov a umožňujú vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených PDF súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

09.10.2019

CVE

CVE-2019-5045, CVE-2019-5046, CVE-2019-5047, CVE-2019-5048, CVE-2019-5050, CVE-2019-5053

Zasiahnuté systémy

NitroPDF

Následky

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

Odporúčania

Na zraniteľnosti v súčasnosti nie sú dostupné aktualizácie. Administrátorom odporúčame sledovať stránky 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.

Zdroje

https://talosintelligence.com/vulnerability_reports/TALOS-2019-0815
https://talosintelligence.com/vulnerability_reports/TALOS-2019-0819
https://talosintelligence.com/vulnerability_reports/TALOS-2019-0817
https://talosintelligence.com/vulnerability_reports/TALOS-2019-0814
https://talosintelligence.com/vulnerability_reports/TALOS-2019-0816
https://talosintelligence.com/vulnerability_reports/TALOS-2019-0830

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

Identifikátor

Google Chrome viacero zraniteľností

Popis

Spoločnosť Google vydala aktualizáciu na svoj internetový prehliadač Google Chrome, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia zraniteľnosť v komponente IndexedDB je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upraveného webového obsahu vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

10.10.2019

CVE

CVE-2019-13693, CVE-2019-13694, CVE-2019-13695, CVE-2019-13696, CVE-2019-13697

Zasiahnuté systémy

Google Chrome verzie staršie ako 77.0.3865.120

Následky

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

Odporúčania

Administrátorom 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/2019/10/stable-channel-update-for-desktop.html
https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-google-chrome-could-allow-for-arbitrary-code-execution_2019-108/
https://www.securityweek.com/google-patches-8-vulnerabilities-chrome-77

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

Identifikátor

Modicon zraniteľnosti

Popis

Bezpečností výskumníci informovali o bezpečnostných zraniteľnostiach v zariadeniach Modicon. Najzávažnejšia bezpečnostná zraniteľnosť v UMAS REST API umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne upravených HTTP požiadaviek spôsobiť zneprístupnenie služieb.

Dátum prvého zverejnenia varovania

10.09.2019

CVE

CVE-2019-6841, CVE-2019-6842, CVE-2019-6843, CVE-2019-6844, CVE-2019-6846, CVE-2019-6847, CVE-2019-6848, CVE-2019-6849, CVE-2019-6850, CVE-2019-6851

Zasiahnuté systémy

Modicon M580
Modicon M340
Modicon Premium
Modicon Quantum
Modicon BMxCRA a 140CRA

Následky

Zneprístupnenie služby
Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame sledovať stránky výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu. Tiež odporúčame aplikovať firewallové pravidlá a blokovať porty 502/TCP a 21/ TCP a deaktivovať službu FTP, pokiaľ nie je potrebná. Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.
Po odstránení zraniteľností, ktoré môžu spôsobiť únik informácií, 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://download.schneider-electric.com/files?p_enDocType=Technical+leaflet&p_File_Name=SEVD-2019-281-03_Modicon_Controllers.pdf&p_Doc_Ref=SEVD-2019-281-03
https://download.schneider-electric.com/files?p_enDocType=Technical+leaflet&p_File_Name=SEVD-2019-281-02_Modicon_Controllers.pdf&p_Doc_Ref=SEVD-2019-281-02
https://talosintelligence.com/vulnerability_reports/TALOS-2019-0868
https://talosintelligence.com/vulnerability_reports/TALOS-2019-0825
https://talosintelligence.com/vulnerability_reports/TALOS-2019-0823
https://talosintelligence.com/vulnerability_reports/TALOS-2019-0827
https://talosintelligence.com/vulnerability_reports/TALOS-2019-0866
https://talosintelligence.com/vulnerability_reports/TALOS-2019-0824
https://talosintelligence.com/vulnerability_reports/TALOS-2019-0847
https://talosintelligence.com/vulnerability_reports/TALOS-2019-0851
https://talosintelligence.com/vulnerability_reports/TALOS-2019-0822
https://talosintelligence.com/vulnerability_reports/TALOS-2019-0867

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.9
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Siemens produkty viacero zraniteľností

Popis

Spoločnosť Siemens vydala bezpečnostné aktualizácie na svoje produkty, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšie zraniteľnosti umožňujú vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne upravených UDP a TCP paketov spôsobiť zneprístupnenie služieb.

Dátum prvého zverejnenia varovania

08.10.2019

CVE

CVE-2017-5715, CVE-2017-5753, CVE-2017-5754, CVE-2018-12126, CVE-2018-12127, CVE-2018-12130, CVE-2018-3615, CVE-2018-3620, CVE-2018-3639, CVE-2018-3640, CVE-2018-3646, CVE-2019-10923, CVE-2019-10936, CVE-2019-11091, CVE-2019-13921, CVE-2019-13929

Zasiahnuté systémy
SIMATIC WinAC RTX 2010 verzie staršie ako SP3
SIMATIC IT UADM verzie staršie ako 1.3
Development/Evaluation Kits for PROFINET IO: DK Standard Ethernet Controller verzie staršie ako 4.1.1 Patch 05
Development/Evaluation Kits for PROFINET IO: EK-ERTEC 200 verzie staršie ako 4.5.0 Patch 01
Development/Evaluation Kits for PROFINET IO: EK-ERTEC 200P verzie staršie ako 4.5.0
CP1616 verzie staršie ako 2.8
CP1604 verzie staršie ako 2.8
SIMATIC CFU PA verzie staršie ako 1.2.0
SIMATIC ET 200AL
SIMATIC ET 200M
SIMATIC ET 200MP IM 155-5 PN BA verzie staršie ako 4.2.3
SIMATIC ET 200MP IM 155-5 PN HF
SIMATIC ET 200MP IM 155-5 PN ST
SIMATIC ET 200S
SIMATIC ET 200SP IM 155-6 PN BA
SIMATIC ET 200SP IM 155-6 PN HA
SIMATIC ET 200SP IM 155-6 PN HF verzie staršie ako 4.2.2
SIMATIC ET 200SP IM 155-6 PN HS
SIMATIC ET 200SP IM 155-6 PN ST
SIMATIC ET 200SP IM 155-6 PN/2 HF verzie staršie ako 4.2.2
SIMATIC ET 200SP IM 155-6 PN/3 HF verzie staršie ako 4.2.1
SIMATIC ET 200ecoPN okrem verzií 6ES7148-6JD00-0AB0 a 6ES7146-6FF00-0AB0
SIMATIC ET 200pro
SIMATIC HMI Comfort Outdoor Panels 7" & 15"
SIMATIC HMI Comfort Panels 4" - 22"
SIMATIC HMI KTP Mobile Panels
SIMATIC PN/PN Coupler
SIMATIC PROFINET Driver verzie staršie ako 2.1
SIMATIC S7-1200 CPU family (incl. F)
SIMATIC S7-1500 CPU family (incl. F) verzie staršie ako 2.0
SIMATIC S7-300 CPU family (incl. F)
SIMATIC S7-400 PN/DP V7 (incl. F)
SIMATIC S7-400 V6 (incl F) a staršie
SIMATIC S7-400H V6 verzie staršie ako 6.0.9
SIMATIC S7-410 V8
SINAMICS DCM verzie staršie ako 1.5 HF1
SINAMICS DCP
SINAMICS G110M V4.7 verzie staršie ako 4.7 SP10 HF5
SINAMICS G120 V4.7 (PN Control Unit) verzie staršie ako 4.7 SP10 HF5
SINAMICS G130 verzie staršie ako 4.7 HF29 a 5.2 HF2
SINAMICS G150 verzie staršie ako 4.8
SINAMICS GH150, GL150, GM150 V4.7 (Control Unit) verzie staršie ako 4.8 SP2 HF9
SINAMICS S110 (Control Unit)
SINAMICS S120 V4.7 verzie staršie ako 4.7 HF34
SINAMICS S150 verzie staršie ako 4.8
SINAMICS SL150 V4.7 (Control Unit)
SINAMICS SM120 V4.7 (Control Unit)
SINUMERIK 828D verzie staršie ako 4.8 SP5
SINUMERIK 840D sl
SCALANCE X-200IRT verzie staršie ako 5.2.1
SIMOTION

Následky
Neoprávnený prístup k citlivým údajom Zneprístupnenie služby

Odporúčania
Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov. Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu. Po odstránení zraniteľností, ktoré môžu spôsobiť únik informácií, 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://cert-portal.siemens.com/productcert/txt/ssa-349422.txt https://cert-portal.siemens.com/productcert/txt/ssa-473245.txt https://cert-portal.siemens.com/productcert/txt/ssa-878278.txt https://cert-portal.siemens.com/productcert/txt/ssa-984700.txt https://cert-portal.siemens.com/productcert/txt/ssa-608355.txt https://www.us-cert.gov/ics/advisories/icsa-19-281-04 https://www.us-cert.gov/ics/advisories/icsa-19-281-03

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

Identifikátor

Phoenix Contact Automationworx Suite zraniteľnosť

Popis

Spoločnosť Phoenix Contact informovala o zraniteľnosti vo svojom produkte Automationworx Suite. Bezpečnostná zraniteľnosť je spôsobená nedostatočným overovaním používateľských vstupov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity dostupnosti systému.

Dátum prvého zverejnenia varovania

15.10.2019

CVE

CVE-2019-16675

Zasiahnuté systémy

Phoenix Contact Automationworx Software Suite verzia 1.86 a staršie

Následky

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

Odporúčania

Výrobca doposiaľ nevydal aktualizáciu riešiacu uvedenú zraniteľnosti.
Odporúčame sledovať stránky výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu. Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy a prílohy z neznámych zdrojov.
Po odstránení zraniteľností, ktoré môžu spôsobiť únik informácií, 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.

Zdroje

https://cert.vde.com/en-us/advisories/vde-2019-016-1

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

Identifikátor

Linux Sudo zraniteľnosť

Popis

Vývojári linuxového nástroja Sudo vydali bezpečnostnú aktualizáciu na svoj produkt, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi eskalovať svoje privilégiá na zasiahnutom systéme.

Dátum prvého zverejnenia varovania

14.10.2019

CVE

CVE-2019-14287

Zasiahnuté systémy

Linuxové distribúcie používajúce Sudo verzie staršie ako 1.8.28

Následky

Eskalácia privilégií

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých systémov. Administrátorom rovnako odporúčame vykonať kontrolu zasiahnutých systémov na prítomnosť nových používateľských účtov a zmenu všetkých hesiel a kľúčov na dotknutých systémoch a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://www.sudo.ws/alerts/minus_1_uid.html
https://www.theregister.co.uk/2019/10/14/linux_sudo_security_bug/
https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=942322
https://thehackernews.com/2019/10/linux-sudo-run-as-root-flaw.html
https://access.redhat.com/security/cve/cve-2019-14287

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

Identifikátor

Dell ImageAssist zraniteľnosť

Popis

Spoločnosť Dell vydala bezpečnostnú aktualizáciu na svoj produkt ImageAssist, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi získať prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

11.10.2019

CVE

CVE-2019-3767

Zasiahnuté systémy

Dell ImageAssist verzie staršie ako 8.7.15

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré môžu spôsobiť únik informácií, 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.dell.com/support/article/sk/sk/skbsd1/sln318831/dsa-2019-139

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

Identifikátor

Zraniteľnosť tlačiarní Samsung

Popis

Spoločnosť Samsung vydala bezpečnostnú aktualizáciu na svoje laserové tlačiarne, ktorá opravuje bezpečnostnú zraniteľnosť.
Bližšie nešpecifikovaná bezpečnostná zraniteľnosť umožňuje vzdialenému, neautentifikovanému útočníkovi spôsobiť zneprístupnenie služieb.

Dátum prvého zverejnenia varovania

02.10.2019

CVE

CVE-2019-6335

Zasiahnuté systémy

Samsung Laser Printers CLP680 verzie staršie ako CLP680DW_V4.00.02.33
M436dn verzie staršie ako V3.82.01.20
M2070
C480

Následky

Zneprístupnenie služieb

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://support.hp.com/hr-en/document/c06461713