BEZPEČNOSTNÝ BULLETIN

Týždeň 11. 08. 2021 - 17. 08. 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-515

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

Identifikátor

Intel produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Intel vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa eskalovať svoje privilégiá a následne získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

10.08.2021

CVE

CVE-2021-0002, CVE-2021-0003, CVE-2021-0004, CVE-2021-0005, CVE-2021-0006, CVE-2021-0007, CVE-2021-0008, CVE-2021-0009, CVE-2021-0012, CVE-2021-0061, CVE-2021-0062, CVE-2021-0083, CVE-2021-0084, CVE-2021-0160, CVE-2021-0196

Zasiahnuté systémy

Intel Ethernet Controllers X722 a 800 Linux RMDA driver vo verzii staršej ako 1.3.19
Intel Ethernet Controllers 800 séria vo verzii staršej ako 1.4.11
Intel NUC 9 Extreme Laptop software driver kit vo verzii staršej ako 2.2.0.20
AverMedia Capture Card Drivers pre Intel NUC Pro Chassis Element vo verzii staršej ako 3.0.64.143
Intel Optane Pmem 200 séria s firmware vo verzii staršej ako 2.2.0.1547
Intel Optane Pmem 100 séria s firmware vo verzii staršej ako 1.2.0.5446
Intel Graphics Windows 10 DCH Drivers vo verzii staršej ako 27.20.100.9030
Intel Graphics Driver pre Windows vo verzii staršej ako 15.45.33.5164
Intel Ethernet Adapters 800 vo verzii staršej ako 1.5.1.0
Intel Ethernet Adapters 800 vo verzii staršej ako 1.5.3.0
Intel Ethernet Adapters 800 vo verzii staršej ako 1.5.4.0

Následky

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

Odporúčania
Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov. Administrátorom odporúčame limitovať prístup k administratívnemu rozhraniu a jeho funkciám zavedením zoznamu pre riadenie prístupov (ACL). Po odstránení zraniteľností, ktoré mohli spôsobiť získanie prístupu k citlivým údajom je dobrou praxou zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00515.html https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00543.html https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00553.html https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00512.html https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00508.html https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00479.html https://us-cert.cisa.gov/ncas/current-activity/2021/08/10/intel-releases-multiple-security-updates

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

Identifikátor

Cognex In-Sight OPC Server - bezpečnostná zraniteľnosť

Popis

Spoločnosť Cognex vydala bezpečnostnú aktualizáciu na produkt In-Sight OPC Server, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom povrhnutia špeciálne vytvorenej webovej stránky, eskalovať svoje privilégiá a následne vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

16.08.2021

CVE

CVE-2021-32935

Zasiahnuté systémy

In-Sight OPC Server vo verzii staršej ako 5.9.2

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.
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-21-224-01

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

Identifikátor

Siemens produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Siemens vydala bezpečnostnú aktualizáciu 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

16.08.2021

CVE

CVE-2020-12357, CVE-2020-12358, CVE-2020-12360, CVE-2020-24486, CVE-2020-24506, CVE-2020-24507, CVE-2020-24511, CVE-2020-24512, CVE-2020-24513, CVE-2020-8670, CVE-2020-8703, CVE-2020-8704, CVE-2020-9272, CVE-2020-9273, CVE-2021-33721, CVE-2021-37178, CVE-2021-37179, CVE-2021-37180

Zasiahnuté systémy

SIMATIC NET CP 1543-1 vo verzii staršej ako v3.0
SINEC NMS vo verzii staršej ako v1.0 SP2
SIMATIC IPC627E s BIOS vo verzii staršej ako v25.02.10
SIMATIC IPC647E s BIOS vo verzii staršej ako v25.02.10
SIMATIC IPC677E s BIOS vo verzii staršej ako v25.02.10
SIMATIC IPC847E s BIOS vo verzii staršej ako v25.02.10
Solid Edge SE2021 vo verzii staršej ako SE2021MP7

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-21-222-07
https://us-cert.cisa.gov/ics/advisories/icsa-21-222-04
https://us-cert.cisa.gov/ics/advisories/icsa-21-222-05
https://us-cert.cisa.gov/ics/advisories/icsa-21-222-08

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

Identifikátor

Microsoft produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Microsoft vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností.

Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvoreného súboru, vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

10.08.2021

CVE

CVE-2021-26428, CVE-2021-26429, CVE-2021-26430, CVE-2021-26433, CVE-2021-34478, CVE-2021-34485, CVE-2021-34532, CVE-2021-36926, CVE-2021-36932, CVE-2021-36933, CVE-2021-36938, CVE-2021-36941, CVE-2021-36949, CVE-2021-36958

Zasiahnuté systémy
.NET Core & Visual Studio ASP .NET Azure Azure Sphere Microsoft Azure Active Directory Connect Microsoft Dynamics Microsoft Graphics Component Microsoft Office Microsoft Office SharePoint Microsoft Office Word Microsoft Scripting Engine Microsoft Windows Codecs Library Remote Desktop Client Windows Bluetooth Service Windows Cryptographic Services Windows Defender Windows Event Tracing Windows Media Windows MSHTML Platform Windows NTLM Windows Print Spooler Components Windows Services for NFS ONCRPC XDR Driver Windows Storage Spaces Controller Windows TCP/IP Windows Update Windows Update Assistant Windows User Profile Service Presnú špecifikáciu jednotlivých zasiahnutých produktov nájdete na webovej adrese: https://msrc.microsoft.com/update-guide/releaseNote/2021-Aug

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

Odporúčania
Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov. Administrátorom odporúčame limitovať prístup k administratívnemu rozhraniu a jeho funkciám zavedením zoznamu pre riadenie prístupov (ACL). 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://msrc.microsoft.com/update-guide/releaseNote/2021-Aug https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-34478 https://us-cert.cisa.gov/ncas/current-activity/2021/08/10/microsoft-releases-august-2021-security-updates

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

Identifikátor

Horner Automation Cscape - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Horner Automation vydala bezpečnostnú aktualizáciu na produkt Cscape, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov 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

16.08.2021

CVE

CVE-2021-32975, CVE-2021-32995, CVE-2021-33015

Zasiahnuté systémy

Cscape vo verzii staršej ako 9.90 SP5

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.
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-21-224-02

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.6
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

CKEditor - bezpečnostná zraniteľnosť

Popis

Vývojári programu CKEditor vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom povrhnutia špeciálne vytvorenej webovej stránky, získať neoprávnený prístup k citlivým údajom a vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

12.08.2021

CVE

CVE-2021-32808

Zasiahnuté systémy

CKEditor vo verzii staršej ako 4.16.2

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

Zdroje

https://ckeditor.com/
https://github.com/ckeditor/ckeditor4/security/advisories/GHSA-6226-h7ff-ch6c
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-32808
https://exchange.xforce.ibmcloud.com/vulnerabilities/207430

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

Identifikátor

Citrix ShareFile - bezpečnostná zraniteľnosť

Popis

Spoločnosť Citrix Systems vydala bezpečnostnú aktualizáciu na svoj produkt ShareFile, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

10.08.2021

CVE

CVE-2021-22932

Zasiahnuté systémy

ShareFile vo verzii staršej ako 5.11.19

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Výrobca odporúča používateľom, ktorí používali CTX269106 mitigation tool aby po aktualizácii programu ShareFile opätovne spustili úlohu šifrovania na pozadí.
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.citrix.com/article/CTX322787
https://us-cert.cisa.gov/ncas/current-activity/2021/08/10/citrix-releases-security-update-sharefile-storage-zones-controller
https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N