BEZPEČNOSTNÝ BULLETIN

Týždeň 12. 10. 2022 - 18. 10. 2022

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-910

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 bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia z bezpečnostných zraniteľností spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

11.10.2022

CVE

CVE-2022-31765, CVE-2022-31766, CVE-2022-37864, CVE-2022-38371, CVE-2022-40147, CVE-2022-40176, CVE-2022-40177, CVE-2022-40178, CVE-2022-40179, CVE-2022-40180, CVE-2022-40181, CVE-2022-40182, CVE-2022-40227, CVE-2022-40631

Zasiahnuté systémy

Siemens Desigo PXM30-1, .E vo verzii staršej ako 02.20.126.11-41
Desigo PXM40-1, .E vo verzii staršej ako 02.20.126.11-41
Desigo PXM50-1, .E vo verzii staršej ako 02.20.126.11-41
PXG3.W100-1 vo verzii staršej ako 02.20.126.11-37
PXG3.W100-2 vo verzii staršej ako 02.20.126.11-41
PXG3.W200-1, 2 vo verzii staršej ako 02.20.126.11-37
RUGGEDCOM RM1224 LTE(4G) EU, NAM vo verzii staršej ako 7.1.2
Solid Edge vo verzii staršej ako SE2022MP9
Nucleus ReadyStart V3 vo verzii staršej ako 2017.02.4 patch "2017.02.4_patch_CVE-2022-38371"
Industrial Edge Management vo verzii staršej ako 1.5.1
RUGGEDCOM RM1224 LTE(4G) EU a NAM vo verzii staršej ako 7.1.2
LOGO! 8 BM vrátane variánt SIPLUS vo verzii staršej ako 8.3
Desingo PXC (viacero verzií)
APOGEE MEC (PPC) BACnet a P2 Ethernet (všetky verzie)
APOGEE MBC (PPC) BACnet a P2 Ethernet (všetky verzie)
TALON TC Compact BACnet (všetky verzie)
TALON TC Modular BACnet (všetky verzie)
SCALANCE (viacero verzií)
SIPLUS NET SCALANCE (viacero verzií)
SIMATIC HMI (viacero verzií)
Nucleus NET (všetky verzie)
Nucleus Source Code (kontaktuje zákaznícke služby Siemens)
Podrobný popis všetkých zasiahnutých verzií sa nachádza v časti Zdroje.

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

Odporúčania
Administrátorom a používateľom odporúčame postupovať podľa odporúčaní výrobcu, ktoré nájdete 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://cert-portal.siemens.com/productcert/html/ssa-360783.html
https://cert-portal.siemens.com/productcert/html/ssa-552702.html
https://cert-portal.siemens.com/productcert/html/ssa-258115.html
https://cert-portal.siemens.com/productcert/html/ssa-313313.html
https://cert-portal.siemens.com/productcert/html/ssa-384224.html
https://cert-portal.siemens.com/productcert/html/ssa-501891.html
https://cert-portal.siemens.com/productcert/html/ssa-649853.html
https://cert-portal.siemens.com/productcert/html/ssa-697140.html
https://cert-portal.siemens.com/productcert/html/ssa-928782.html
https://cert-portal.siemens.com/productcert/html/ssb-898115.html
https://cert-portal.siemens.com/productcert/html/ssa-935500.html

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

Identifikátor

Adobe Dimension, Acrobat a Acrobat Reader - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Adobe vydala bezpečnostné aktualizácie na svoje produkty Dimension, Acrobat a Acrobat Reader, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšie z uvedených zraniteľností spočívajú v nedostatočnej implementácii bezpečnostných mechanizmov a umožňujú lokálnemu, autentifikovanému útočníkovi vykonať škodlivý kód s následkom narušenia dôvernosti, integrity a dostupnosti systému v medziach práv prihláseného používateľa.

Dátum prvého zverejnenia varovania

11.10.2022

CVE

CVE-2022-35691, CVE-2022-38437, CVE-2022-38440, CVE-2022-38441, CVE-2022-38442, CVE-2022-38443, CVE-2022-38444, CVE-2022-38445, CVE-2022-38446, CVE-2022-38447, CVE-2022-38448, CVE-2022-38449, CVE-2022-38450, CVE-2022-42339, CVE-2022-42342

Zasiahnuté systémy

Adobe Dimension vo verzii staršej ako 3.4.6
Adobe Acrobat DC Continuous vo verzii staršej ako 22.003.20258
Adobe Acrobat Reader DC Continuous vo verzii staršej ako 22.003.20258
Adobe Acrobat 2020 Classic 2020 vo verzii staršej ako 20.005.30407
Adobe Acrobat Reader 2020 Classic vo verzii staršej ako 2020 20.005.30407

Následky

Neoprávnený prístup k citlivým údajom
Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Administrátorom a používateľom odporúčame nainštalovať bezpečnostné aktualizácie.
Taktiež odporúčame neotvárať správy, URL odkazy a súbory pochádzajúce z neznámych zdrojov.
Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu 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://helpx.adobe.com/security/products/dimension/apsb22-57.html
https://helpx.adobe.com/security/products/acrobat/apsb22-46.html

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 bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia z bezpečnostných zraniteľností spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

11.10.2022

CVE

CVE-2022-31765, CVE-2022-31766, CVE-2022-37864, CVE-2022-38371, CVE-2022-40147, CVE-2022-40176, CVE-2022-40177, CVE-2022-40178, CVE-2022-40179, CVE-2022-40180, CVE-2022-40181, CVE-2022-40182, CVE-2022-40227, CVE-2022-40631

Zasiahnuté systémy

Siemens Desigo PXM30-1, .E vo verzii staršej ako 02.20.126.11-41
Desigo PXM40-1, .E vo verzii staršej ako 02.20.126.11-41
Desigo PXM50-1, .E vo verzii staršej ako 02.20.126.11-41
PXG3.W100-1 vo verzii staršej ako 02.20.126.11-37
PXG3.W100-2 vo verzii staršej ako 02.20.126.11-41
PXG3.W200-1, 2 vo verzii staršej ako 02.20.126.11-37
RUGGEDCOM RM1224 LTE(4G) EU, NAM vo verzii staršej ako 7.1.2
Solid Edge vo verzii staršej ako SE2022MP9
Siemens Industrial Edge Management vo verzii staršej ako 1.5.1
Industrial Edge Management vo verzii staršej ako 1.5.1
RUGGEDCOM RM1224 LTE(4G) EU a NAM vo verzii staršej ako 7.1.2
LOGO! 8 BM vrátane variánt SIPLUS vo verzii staršej ako 8.3
Desingo PXC (viacero verzií)
APOGEE MEC (PPC) BACnet a P2 Ethernet (všetky verzie)
APOGEE MBC (PPC) BACnet a P2 Ethernet (všetky verzie)
TALON TC Compact BACnet (všetky verzie)
TALON TC Modular BACnet (všetky verzie)
SCALANCE (viacero verzií)
SIPLUS NET SCALANCE (viacero verzií)
SIMATIC HMI (viacero verzií)
Nucleus NET (všetky verzie)
Nucleus Source Code (kontaktuje zákaznícke služby Siemens)
Nucleus ReadyStart V3 vo verzii staršej ako 2017.02.6
Podrobný popis všetkých zasiahnutých verzií sa nachádza v časti Zdroje.

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

Odporúčania
Administrátorom a používateľom odporúčame vykonať bezodkladnú aktualizáciu zasiahnutých systémov. V prípade, že sa zraniteľnosť týka všetkých verzií zasiahnutých systémov, odporúčame postupovať podľa návodov na mitigáciu zraniteľností, ktoré sa nachádzajú sa v časti Zdroje. Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu 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/html/ssa-360783.html https://cert-portal.siemens.com/productcert/html/ssa-552702.html https://cert-portal.siemens.com/productcert/html/ssa-258115.html https://cert-portal.siemens.com/productcert/html/ssa-313313.html https://cert-portal.siemens.com/productcert/html/ssa-384224.html https://cert-portal.siemens.com/productcert/html/ssa-501891.html https://cert-portal.siemens.com/productcert/html/ssa-649853.html https://cert-portal.siemens.com/productcert/html/ssa-697140.html https://cert-portal.siemens.com/productcert/html/ssa-928782.html https://cert-portal.siemens.com/productcert/html/ssb-898115.html https://cert-portal.siemens.com/productcert/html/ssa-935500.html https://www.cisa.gov/uscert/ics/advisories/icsa-22-286-02 https://www.cisa.gov/uscert/ics/advisories/icsa-22-286-07

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

Identifikátor

Google Chrome - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Google vydala bezpečnostnú aktualizáciu na internetový prehliadač Chrome, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia zraniteľnosť sa nachádza v open source 2D grafickej knižnici Skia, spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi vykonať škodlivý kód s následkom narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

11.10.2022

CVE

CVE-2022-3445, CVE-2022-3446, CVE-2022-3447, CVE-2022-3448, CVE-2022-3449, CVE-2022-3450

Zasiahnuté systémy

Google Chrome vo verzii staršej ako 106.0.5249.119

Následky

Neoprávnený prístup k citlivým údajom
Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Administrátorom a používateľom odporúčame nainštalovať bezpečnostné aktualizácie.
Taktiež odporúčame neotvárať správy, URL odkazy a súbory pochádzajúce z neznámych zdrojov.
Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu 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://chromereleases.googleblog.com/2022/10/stable-channel-update-for-desktop_11.html
https://community.qualys.com/vulnerability-detection-pipeline/

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

Identifikátor

IBM InfoSphere Information Server - bezpečnostná zraniteľnosť

Popis

Spoločnosť IBM vydala bezpečnostné aktualizácie na svoj produkt InfoSphere Information Server, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvoreného XML dokumentu získať neoprávnený prístup k citlivým údajom a alebo spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

17.10.2022

CVE

CVE-2022-40747

Zasiahnuté systémy

IBM InfoSphere Information Server vo verzii staršej ako 11.7.1.0
IBM InfoSphere Information Server vo verzii staršej ako 11.7.1.4

Následky

Neoprávnený prístup k citlivým údajom
Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom 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 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.ibm.com/support/pages/node/6829373
https://exchange.xforce.ibmcloud.com/vulnerabilities/236584

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

Identifikátor

Palo Alto Networks PAN-OS - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Palo Alto Networks vydala bezpečnostnú aktualizáciu na svoj produkt PAN-OS 8, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii mechanizmov autentifikácie a umožňuje vzdialenému, neautentifikovanému útočníkovi vykonať škodlivý kód s následkom narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

12.10.2022

CVE

CVE-2022-0030

Zasiahnuté systémy

Palo Alto Networks PAN-OS 8 vo verzii staršej ako 8.1.24

Následky

Neoprávnený prístup do systému
Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Administrátorom a používateľom odporúčame nainštalovať bezpečnostné aktualizácie.
Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu 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://security.paloaltonetworks.com/CVE-2022-0030

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

Identifikátor

Zoom produkty - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť Zoom Video Communications vydala bezpečnostné aktualizácie na svoje produkty Zoom a na Zoom On-Premise Meeting Connector MMR, ktorá opravuje dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť sa nachádza v aplikácii Zoom client pre macOS, spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právami používateľa získať úplnu kontrolu nad Zoom Apps doplnkami bežiacimi v Zoom klientovi.

Dátum prvého zverejnenia varovania

17.10.2022

CVE

CVE-2022-28761, CVE-2022-28762

Zasiahnuté systémy

Zoom Video Communications Zoom Client pre macOS (Štarndard aj IT Admin) od 5.10.6 a verzie staršie ako 5.12.0
Zoom Video Communications Zoom On-Premise Meeting Connector MMR vo verzii staršej ako 4.8.20220916.131

Následky

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 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-2022-28762
https://www.securityweek.com/zoom-macos-contains-high-risk-security-flaw

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

Identifikátor

Linux kernel - päť bezpečnostných zraniteľností

Popis

Vývojári jadra operačného systému Linux vydali bezpečnostnú aktualizáciu, ktorá opravuje päť bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právami používateľa prostredníctvom podvrhnutia špeciálne vytvorených WLAN rámcov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

17.10.2022

CVE

CVE-2022-41674, CVE-2022-42719, CVE-2022-42720, CVE-2022-42721, CVE-2022-42722

Zasiahnuté systémy

Linux kernel vo verzii staršej ako 5.19.16

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 zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://www.openwall.com/lists/oss-security/2022/10/13/2
https://nvd.nist.gov/vuln/detail/CVE-2022-41674
https://nvd.nist.gov/vuln/detail/CVE-2022-42719
https://nvd.nist.gov/vuln/detail/CVE-2022-42720
https://nvd.nist.gov/vuln/detail/CVE-2022-42721
https://nvd.nist.gov/vuln/detail/CVE-2022-42722

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

Identifikátor

Hitachi Energy Lumada Asset Performance Management - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť Hitachi Energy vydala bezpečnostné aktualizácie na svoj produkt Lumada Asset Performance Management, ktoré opravujú dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť sa nachádza v službe Prognostic Model Executor, spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právami používateľa vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

13.10.2022

CVE

CVE-2022-22950, CVE-2022-22965

Zasiahnuté systémy

Hitachi Energy Lumada Asset Performance Manager (APM) vo verzii staršej ako 6.0.0.5
Hitachi Energy Lumada Asset Performance Manager (APM) vo verzii staršej ako 6.1.0.2
Hitachi Energy Lumada Asset Performance Manager (APM) vo verzii staršej ako 6.2.0.4
Hitachi Energy Lumada Asset Performance Manager (APM) vo verzii staršej ako 6.3.0.3

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame vykonať bezodkladnú aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu 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/uscert/ics/advisories/icsa-22-286-05