BEZPEČNOSTNÝ BULLETIN

Týždeň 06. 01. 2021 - 12. 01. 2021

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Viacero bezpečnostných zraniteľností v produktoch Microsoft	Vysoká	**8.8**
02.	Viacero bezpečnostných zraniteľností v produktoch Adobe	Vysoká	**8.8**
03.	Bezpečnostné zraniteľnosti v produkte Schneider Electric EcoStruxure Power Build - Rapsody	Vysoká	**7.8**
04.	Bezpečnostná zraniteľnosť v produktoch Delta Electronics CNCSoft ScreenEditor, DOPSoft a CNCSoft-B	Vysoká	**7.8**
05.	Bezpečnostná zraniteľnosť v produkte Omron CX-One	Vysoká	**7.8**
06.	Bezpečnostná zraniteľnosť v produktoch SOOIL Dana Diabecare RS	Vysoká	**7.6**
07.	Bezpečnostné zraniteľnosti v produkte Eaton EASYsoft	Stredná	**5.8**
08.	Bezpečnostná zraniteľnosť v produkte Innokas Yhtymä Oy Vital Signs Monitor	Stredná	**5.3**

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:
01439/2020/SK-CERT-296

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

Identifikátor

Viacero bezpečnostných zraniteľností v produktoch Microsoft

Popis

Spoločnosť Microsoft vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť sa nachádza v produkte Windows Remote Desktop, je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.
Jedna zo zraniteľností je v súčasnosti aktívne zneužívaná útočníkmi.

Dátum prvého zverejnenia varovania

12.01.2021

CVE

CVE-2020-26870, CVE-2021-1636, CVE-2021-1637, CVE-2021-1643, CVE-2021-1644, CVE-2021-1645, CVE-2021-1647, CVE-2021-1648, CVE-2021-1656, CVE-2021-1663, CVE-2021-1669, CVE-2021-1670, CVE-2021-1672, CVE-2021-1676, CVE-2021-1677, CVE-2021-1694, CVE-2021-1696, CVE-2021-1699, CVE-2021-1707, CVE-2021-1708, CVE-2021-1711, CVE-2021-1713, CVE-2021-1714, CVE-2021-1715, CVE-2021-1716, CVE-2021-1725

Zasiahnuté systémy

Microsoft Visual Studio 2017, 2019
Microsoft SQL Server 2012, 2014, 2016, 2017, 2019
Windows Server 2008, 2012 R2, 2016, 2019
Windows 7, 8.1, 10
HEVC Video Extensions všetky verzie
Windows Defender všetky verzie
Microsoft Remote Desktop všetky verzie
Remote Desktop client pre Windows Desktop všetky verzie
Microsoft Remote Desktop pre Android všetky verzie
Microsoft Azure Kubernetes Service všetky verzie
Microsoft SharePoint 2010, 2013
Microsoft SharePoint Server 2019
Microsoft SharePoint Enterprise Server 2016
Microsoft 365 Apps pre Enterprise
Microsoft Office 2010, 2013, 2016, 2019
Microsoft Office Web Apps Server 2013 Service Pack 1
Microsoft Excel 2010, 2013, 2016
Microsoft Office Online Server
Microsoft Office 2019 pre Mac
Excel Services
Microsoft Word 2010, 2013, 2016
Microsoft Office Web Apps Server 2013 Service Pack 1
Bot Framework SDK pre Python
Bot Framework SDK pre JavaScript
Bot Framework SDK pre .NET Framework
Presnú specifikáciu verzií jednotlivých zasiahnutých produktov nájdete na stránke:
https://msrc.microsoft.com/update-guide/releaseNote/2021-Jan

Následky

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

Odporúčania

Administrátorom a používateľom 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://msrc.microsoft.com/update-guide/releaseNote/2021-Jan
https://www.securityweek.com/microsoft-patch-tuesday-83-vulnerabilities-10-critical-1-actively-exploited
https://www.zdnet.com/article/microsoft-fixes-defender-zero-day-in-january-2021-patch-tuesday/

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

Identifikátor

Viacero bezpečnostných zraniteľností v produktoch Adobe

Popis

Spoločnosť Adobe vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť sa nachádza v produkte Photoshop, je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

12.01.2021

CVE

CVE-2021-21006, CVE-2021-21007, CVE-2021-21008, CVE-2021-21009, CVE-2021-21010, CVE-2021-21011, CVE-2021-21012, CVE-2021-21013

Zasiahnuté systémy

Adobe Photoshop 2021 vo verzii staršej ako 22.1
Adobe Illustrator 2020 vo verzii staršej ako 25.1
Adobe Animate vo verzii staršej ako 21.0.2
Adobe Campaign Classic vo verzii staršej ako Gold Standard 11
Adobe Campaign Classic vo verzii staršej ako 20.3.3 - Build 9234
Adobe Campaign Classic vo verzii staršej ako 20.2.4 - Build 9187
Adobe Campaign Classic vo verzii staršej ako 20.1.4 - Build 9126
Adobe Campaign Classic vo verzii staršej ako 19.2.4 - Build 9082
Adobe Campaign Classic vo verzii staršej ako 19.1.8 - Build 9039
Adobe InCopy vo verzii staršej ako 16.0
Adobe Captivate 2019 vo verzii staršej ako 11.5.1.499 (vrátane)
Adobe Bridge vo verzii staršej ako 11.0.1

Následky

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

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 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.zdnet.com/article/adobe-patches-code-execution-vulnerabilities-in-the-first-security-update-of-2021/ https://threatpost.com/adobe-critical-flaws-flash-player/162958/ https://www.cybersecurity-help.cz/vdb/SB2021011241

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

Identifikátor

Bezpečnostné zraniteľnosti v produkte Schneider Electric EcoStruxure Power Build - Rapsody

Popis

Spoločnosť Schneider Electric vydala bezpečnostnú aktualizáciu na svoj produkt EcoStruxure Power Build - Rapsody, ktorá opravuje dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom podvrhnutia škodlivého SSD súbora vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

12.01.2021

CVE

CVE-2021-22697, CVE-2021-22698

Zasiahnuté systémy

EcoStruxure Power Build - Rapsody software všetky verzie vrátane 2.1.13

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.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od Internetu.
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://us-cert.cisa.gov/ics/advisories/icsa-21-012-01

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

Identifikátor

Bezpečnostná zraniteľnosť v produktoch Delta Electronics CNCSoft ScreenEditor, DOPSoft a CNCSoft-B

Popis

Spoločnosť Delta Electronics vydala bezpečnostné aktualizácie na svoje produkty CNCSoft ScreenEditor, DOPSoft a CNCSoft-B, ktoré opravujú viacero bezpečnostných zraniteľností.
Bezpečnostné zraniteľnosti spočívajú v nedostatočnej implementácii bezpečnostných mechanizmov a umožňujú lokálnemu, neautentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

07.01.2021

CVE

CVE-2020-27275, CVE-2020-27277, CVE-2020-27281, CVE-2020-27287, CVE-2020-27289, CVE-2020-27291, CVE-2020-27293

Zasiahnuté systémy

CNCSoft ScreenEditor verzie staršie ako v1.01.28
DOPSoft verzie staršie ako v4.00.10.17
CNCSoft-B verzie staršie ako v1.0.0.3

Následky

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

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 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://us-cert.cisa.gov/ics/advisories/icsa-21-005-06
https://us-cert.cisa.gov/ics/advisories/icsa-21-005-05
https://us-cert.cisa.gov/ics/advisories/icsa-21-007-04

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

Identifikátor

Bezpečnostná zraniteľnosť v produkte Omron CX-One

Popis

Spoločnosť Omron vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou 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

07.01.2021

CVE

CVE-2020-27257, CVE-2020-27259, CVE-2020-27261

Zasiahnuté systémy

CX-Protocol vo verzii staršej ako 2.03
CX-Server vo verzii staršej ako 5.0.28
CX-Position vo verzii staršej ako 2.52

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od Internetu.
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://us-cert.cisa.gov/ics/advisories/icsa-21-007-02

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

Identifikátor

Bezpečnostná zraniteľnosť v produktoch SOOIL Dana Diabecare RS

Popis

Spoločnosť SOOIL Developments vydala bezpečnostnú aktualizáciu na svoje produkty Dana Diabecare RS a AnyDana, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v existencii zabudovaného používateľského účtu s predvoleným heslom a umožňuje neautentifikovanému útočníkovi, ktorý sa nachádza v rovnakom sieťovom segmente, vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

12.01.2021

CVE

CVE-2020-27256, CVE-2020-27258, CVE-2020-27264, CVE-2020-27266, CVE-2020-27268, CVE-2020-27269, CVE-2020-27270, CVE-2020-27272, CVE-2020-27276

Zasiahnuté systémy

Dana Diabecare RS: vo verzii staršej ako 3.0
AnyDana-i: vo verzii staršej ako 3.0
AnyDana-A: vo verzii staršej ako 3.0

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnený prístup do systému
Neoprávnená zmena v systéme

Odporúčania

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

Zdroje

https://us-cert.cisa.gov/ics/advisories/icsma-21-012-01

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 5.8
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Bezpečnostné zraniteľnosti v produkte Eaton EASYsoft

Popis

Spoločnosť Eaton vydala bezpečnostnú aktualizáciu na svoj produkt EASYsoft, ktorá opravuje dve bezpečnostné zraniteľnosti.
Zraniteľnosti spočívajú v nedostatočnej implementácii bezpečnostných mechanizmov a umožňujú lokálnemu neautentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

07.01.2021

CVE

CVE-2020-6655, CVE-2020-6656

Zasiahnuté systémy

EASYsoft vo verzii staršej ako 7.20 (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.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.
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://us-cert.cisa.gov/ics/advisories/icsa-21-007-03

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 5.3
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Bezpečnostná zraniteľnosť v produkte Innokas Yhtymä Oy Vital Signs Monitor

Popis

Spoločnosť Innokas Yhtymä Oy vydala bezpečnostnú aktualizáciu na svoj produkt Vital Signs Monitor, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť umožňuje neautentifikovanému, lokálnemu útočníkovi s fyzickým prístupom k zariadeniu vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

07.01.2021

CVE

CVE-2020-27260, CVE-2020-27262

Zasiahnuté systémy

Innokas Yhtymä Oy Vital Signs Monitor VC150 vo verzii staršej ako 1.7.15b

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme

Odporúčania

Administrátorom 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://us-cert.cisa.gov/ics/advisories/icsma-21-007-01