BEZPEČNOSTNÝ BULLETIN

Týždeň 05. 01. 2022 - 11. 01. 2022

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	MediaWiki - bezpečnostná zraniteľnosť	Vysoká	**8.0**
02.	WordPress - bezpečnostná zraniteľnosť	Vysoká	**8.0**
03.	Omron CX-One produkt - bezpečnostná zraniteľnosť	Vysoká	**7.8**
04.	VMware Workstation,Fusion a ESXi produkty - bezpečnostná zraniteľnosť	Vysoká	**7.7**
05.	IDEC PLCs - viacero bezpečnostných zraniteľností	Vysoká	**7.6**
06.	Fernhill SCADA Server - bezpečnostná zraniteľnosť	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:
01439/2020/SK-CERT-650

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

Identifikátor

MediaWiki - bezpečnostná zraniteľnosť

Popis

Vývojári nástroja MediaWiki 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 zasielania špeciálne vytvorenej požiadavky, vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

07.01.2022

CVE

CVE-2021-46147

Zasiahnuté systémy

MediaWiki vo verzii staršej ako 1.35.5
MediaWiki vo verzii staršej ako 1.36.3
MediaWiki vo verzii staršej ako 1.37.1

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.

Zdroje

https://phabricator.wikimedia.org/T293341
https://www.mediawiki.org/wiki/MediaWiki
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-46147
https://exchange.xforce.ibmcloud.com/vulnerabilities/216873

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

Identifikátor

WordPress - bezpečnostná zraniteľnosť

Popis

Vývojári nástroja WordPress 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, vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

06.01.2022

CVE

CVE-2022-21662

Zasiahnuté systémy

WordPress vo verzii staršej ako 5.8.3

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.
Pri webových stránkach odporúčame zvážiť možnosť prevádzkovať redakčný systém nedostupný z verejného internetu a na verejný prezentačný server nahrávať len vyexportovanú statickú verziu stránky.

Zdroje

https://wordpress.org/news/2022/01/wordpress-5-8-3-security-release/
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21662
https://exchange.xforce.ibmcloud.com/vulnerabilities/216859
https://www.cyberkendra.com/2022/01/wordpress-core-vulnerabilities-puts.html
https://www.securityweek.com/wordpress-583-patches-several-injection-vulnerabilities
https://www.bleepingcomputer.com/news/security/wordpress-583-security-update-fixes-sql-injection-xss-flaws/

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

Identifikátor

Omron CX-One produkt - bezpečnostná zraniteľnosť

Popis

Spoločnosť Omron vydala bezpečnostnú aktualizáciu na produkt CX-One, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom povrhnutia špeciálne vytvorených súborov, vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

06.01.2022

CVE

CVE-2022-21137

Zasiahnuté systémy

CX-Server vo verzii staršej ako 5.0.29.2

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.
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-22-006-01

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.7**
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

VMware Workstation,Fusion a ESXi produkty - bezpečnostná zraniteľnosť

Popis

Spoločnosť VMware vydala bezpečnostnú aktualizáciu na produkty Workstation,Fusion a ESXi, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej požiadavky, vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

04.01.2022

CVE

CVE-2021-22045

Zasiahnuté systémy

VMware ESXi vo verzii staršej ako ESXi670-202111101-SG
VMware ESXi vo verzii staršej ako ESXi650-202110101-SG
VMware ESXi vo verzii staršej ako 7.0 (vrátane)
VMware Fusion vo verzii staršej ako 12.2.0
VMware Workstation vo verzii staršej ako 16.2.0

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).

Zdroje

https://www.vmware.com/security/advisories/VMSA-2022-0001.html
https://www.zerodayinitiative.com/advisories/ZDI-22-003/
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-22045
https://exchange.xforce.ibmcloud.com/vulnerabilities/216594

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

Identifikátor

IDEC PLCs - viacero bezpečnostných zraniteľností

Popis

Spoločnosť IDEC vydala bezpečnostnú aktualizáciu na svoje PLC produkty, ktorá opravuje viacero bezpečnostných zraniteľností. Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje neautentifikovanému útočníkovi, ktorý sa nachádza v rovnakom sieťovom segmente eskalovať svoje privilégiá a následne získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

06.01.2022

CVE

CVE-2021-20826, CVE-2021-20827, CVE-2021-37400, CVE-2021-37401

Zasiahnuté systémy

FC6A MICROSmart All-in-One CPU Module vo verzii staršej ako v2.40
FC6B MICROSmart All-in-One CPU Module vo verzii staršej ako v2.40
FC6A MICROSmart Plus CPU Module vo verzii staršej ako v2.00
FC6B MICROSmart Plus CPU Module vo verzii staršej ako v2.40
FT1A Controller SmartAXIS Pro/Lite vo verzii staršej ako v2.40
WindLDR vo verzii staršej ako v8.20.0
WindEDIT Lite vo verzii staršej ako v1.4.0
Data File Manager vo verzii staršej ako v2.13.0

Následky

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

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

Zdroje

https://us-cert.cisa.gov/ics/advisories/icsa-22-006-03

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

Identifikátor

Fernhill SCADA Server - bezpečnostná zraniteľnosť

Popis

Spoločnosť Fernhill vydala bezpečnostnú aktualizáciu na produkt SCADA Server, ktorá opravuje bezpečnostnú zraniteľnosť. 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

06.01.2022

CVE

CVE-2022-21155

Zasiahnuté systémy

Fernhill SCADA Server vo verzii staršej ako 3.78

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-22-006-02