BEZPEČNOSTNÝ BULLETIN

Týždeň 17. 03. 2021 - 23. 03. 2021

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	WP Super Cache a Tutor LMS pluginy pre Wordpress - viacero zraniteľností	Vysoká	**8.8**
02.	NetApp produkty - bezpečnostná zraniteľnosť	Vysoká	**8.6**
03.	TYPO3 - viacero zraniteľností	Vysoká	**8.1**
04.	Adobe Acrobat a Adobe Reader - tri bezpečnostné zraniteľnosti	Vysoká	**7.8**
05.	Nbdkit libnbd - bezpečnostná zraniteľnosť	Vysoká	**7.5**
06.	Facebook mvfst a proxygen - bezpečnostná zraniteľnosť	Vysoká	**7.5**
07.	HP Enterprise Network Orchestrator - bezpečnostná zraniteľnosť	Vysoká	**7.5**
08.	Moodle - viacero zraniteľností	Vysoká	**7.2**
09.	Cisco RV132W a RV134W produkty - bezpečnostná zraniteľnosť	Vysoká	**7.2**
10.	Junos OS EX, QFX, MX, SRX - bezpečnostná zraniteľnosť	Stredná	**6.5**
11.	Hitachi ABB Power Grids série AFS - bezpečnostná zraniteľnosť	Stredná	**6.5**

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-368

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

Identifikátor

WP Super Cache a Tutor LMS pluginy pre Wordpress - viacero zraniteľností

Popis

Vývojári pluginov WP Super Cache a Tutor LMS vydali bezpečnostné aktualizácie svojich produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi prostredníctvom zasielania špeciálne vytvorenej HTTP požiadavky vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

16.03.2021

CVE

-

Zasiahnuté systémy

WP Super Cache vo verzii staršej ako 1.7.2
Tutor LMS vo verzii staršej ako v.1.8.3

Následky

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

Odporúčania

Odporúčame uistiť sa, či Vaše stránky nevyužívajú pluginy v zraniteľných verziách. V prípade, že áno, administrátorom 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.

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/198335
https://wordpress.org/plugins/wp-super-cache/
https://patchstack.com/database/vulnerability/wp-super-cache/wordpress-wp-super-cache-plugin-1-7-1-authenticated-remote-code-execution-rce-vulnerability
https://thehackernews.com/2021/03/flaws-in-two-popular-wordpress-plugins.html
https://www.cybersafe.news/flaws-in-wordpress-plugins-affect-over-7m-websites/
https://threatpost.com/tutor-lms-wordpress-security-holes/164868/
https://www.wordfence.com/blog/2021/03/several-vulnerabilities-patched-in-tutor-lms-plugin/
https://wpguynews.com/wp-super-cache-vulnerability-affects-over-2-million-sites-via-martinibuster/

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

Identifikátor

NetApp produkty - bezpečnostná zraniteľnosť

Popis

Spoločnosť NetApp vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne vytvorenej HTTP požiadavky vykonať škodlivý kód, získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

15.03.2021

CVE

CVE-2021-26987

Zasiahnuté systémy

NetApp Element Plug-in pre vCenter Server vo verzii staršej ako 2.17.56
NetApp Management Services pre Element Software a NetApp HCI vo verzii staršej ako 2.17.56
NetApp NetApp SolidFire HCI Management Node vo verzii staršej ako 12.2 (vrátane)

Následky

Vykonanie škodlivého kódu
Zneprístupnenie služby
Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme

Odporúčania

Administrátorom 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.

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/198274
https://security.netapp.com/advisory/ntap-20210315-0001/

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

Identifikátor

TYPO3 - viacero zraniteľností

Popis

Vývojári CMS TYPO3 vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii mechanizmov autentifikácie a umožňuje vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

16.03.2021

CVE

CVE-2021-21339, CVE-2021-21340, CVE-2021-21358, CVE-2021-21359, CVE-2021-21370, CVE-2021-28380, CVE-2021-28381

Zasiahnuté systémy

TYPO3 vo verzii staršej ako 6.2.57
TYPO3 vo verzii staršej ako 7.6.51
TYPO3 vo verzii staršej ako 8.7.40
TYPO3 vo verzii staršej ako 9.5.25
TYPO3 vo verzii staršej ako 10.4.14
TYPO3 vo verzii staršej ako 11.1.1

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme
Zneprístupnenie služby

Odporúčania

Odporúčame uistiť sa, či Vaše stránky nie sú založené na frameworku TYPO3. V prípade, že áno, 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://exchange.xforce.ibmcloud.com/vulnerabilities/198296
https://typo3.org/security/advisory/typo3-core-sa-2021-006
https://exchange.xforce.ibmcloud.com/vulnerabilities/198279
https://exchange.xforce.ibmcloud.com/vulnerabilities/198280
https://exchange.xforce.ibmcloud.com/vulnerabilities/198283
https://exchange.xforce.ibmcloud.com/vulnerabilities/198284
https://exchange.xforce.ibmcloud.com/vulnerabilities/198298

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

Identifikátor

Adobe Acrobat a Adobe Reader - tri bezpečnostné zraniteľnosti

Popis

Spoločnosť Adobe vydala bezpečnostné aktualizácie na produkty Adobe Acrobat a Adobe Reader, ktoré opravujú tri bezpečnostné zraniteľnosti.

Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov 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

17.03.2021

CVE

CVE-2021-21086, CVE-2021-21088, CVE-2021-21089

Zasiahnuté systémy

Adobe Acrobat 2017 vo verzii staršej ako 2017.011.30190
Adobe Acrobat Reader 2017 vo verzii staršej ako 2017.011.30190
Adobe Acrobat 2020 vo verzii staršej ako 2020.001.30020
Adobe Acrobat Reader 2020 vo verzii staršej ako 2020.001.30020
Adobe Acrobat DC vo verzii staršej ako 2021.001.20135
Adobe Acrobat Reader DC vo verzii staršej ako 2021.001.20135

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému
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 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.zerodayinitiative.com/advisories/ZDI-21-335/
https://exchange.xforce.ibmcloud.com/vulnerabilities/198387

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

Identifikátor

Nbdkit libnbd - bezpečnostná zraniteľnosť

Popis

Vývojári nástroja Nbdkit vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť v knižnici libnbd.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

15.03.2021

CVE

CVE-2021-20286

Zasiahnuté systémy

libnbd vo verzii staršej ako 1.7.3

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/198272
https://bugzilla.redhat.com/show_bug.cgi?id=1934727
https://gitlab.com/nbdkit/libnbd/-/commit/fb4440de9cc76e9c14bd3ddf3333e78621f40ad0
https://github.com/libguestfs/nbdkit

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

Identifikátor

Facebook mvfst a proxygen - bezpečnostná zraniteľnosť

Popis

Spoločnosť Facebook vydala bezpečnostné aktualizácie na produkty mvfst a proxygen, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne vytvorenej požiadavky spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

15.03.2021

CVE

CVE-2021-24029

Zasiahnuté systémy

mvfst vo verzii staršej ako a67083ff4b8dcbb7ee2839da6338032030d712b0
proxygen vo verzii staršej ako v2021.03.15.00.

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/198250
https://www.facebook.com/security/advisories/cve-2021-24029
https://github.com/facebookincubator/mvfst
https://docs.hhvm.com/hhvm/basic-usage/proxygen

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

Identifikátor

HP Enterprise Network Orchestrator - bezpečnostná zraniteľnosť

Popis

Spoločnosť HP vydala bezpečnostnú aktualizáciu na svoj produkt Enterprise Network Orchestrator, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom SQL injekcie získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

16.03.2021

CVE

CVE-2021-26578

Zasiahnuté systémy

HP Enterprise Network Orchestrator vo verzii staršej ako 2.5

Následky

Neoprávnený prístup k citlivým údajom

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://support.hpe.com/hpesc/public/docDisplay?docId=hpesbgn04097en_us
https://www.zerodayinitiative.com/advisories/ZDI-21-337/

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.2
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Moodle - viacero zraniteľností

Popis

Vývojári systému Moodle vydali bezpečnostné aktualizácie svojho produktu, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup k citlivým údajom a vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

15.03.2021

CVE

CVE-2021-20279, CVE-2021-20280, CVE-2021-20281, CVE-2021-20282, CVE-2021-20283

Zasiahnuté systémy

Moodle vo verzii staršej ako 3.10.2
Moodle vo verzii staršej ako 3.9.5
Moodle vo verzii staršej ako 3.8.8
Moodle vo verzii staršej ako 3.5.17

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://exchange.xforce.ibmcloud.com/vulnerabilities/198259
https://moodle.org/mod/forum/discuss.php?d=419650

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.2
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Cisco RV132W a RV134W produkty - bezpečnostná zraniteľnosť

Popis

Spoločnosť Cisco vydala bezpečnostné aktualizácie na produkty RV132W a RV134W, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, autentifikovanému útočníkovi prostredníctvom zasielania špeciálne vytvorenej HTTP požiadavky vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

17.03.2021

CVE

CVE-2021-1287

Zasiahnuté systémy

Cisco RV132W ADSL2+ Wireless-N VPN routery s firmware vo verzii staršej ako 1.0.1.15
Cisco RV134W VDSL2 Wireless-AC VPN routery s firmware vo verzii staršej ako 1.0.1.21

Následky

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

Odporúčania

Administrátorom 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.

Zdroje

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-132w134w-overflow-Pptt4H2p
https://threatpost.com/cisco-security-hole-small-business-routers/164859/

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 6.5
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Junos OS EX, QFX, MX, SRX - bezpečnostná zraniteľnosť

Popis

Spoločnosť Juniper Networks vydala bezpečnostné aktualizácie na svoj produkt Junos OS, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje neautentifikovanému útočníkovi, ktorý sa nachádza v rovnakom sieťovom segmente, spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

16.03.2021

CVE

CVE-2021-0215

Zasiahnuté systémy

Juniper Networks Junos OS vo verzii staršej ako 14.1X53-D54
Juniper Networks Junos OS vo verzii staršej ako 15.1X49-D240
Juniper Networks Junos OS vo verzii staršej ako 15.1X53-D593
Juniper Networks Junos OS vo verzii staršej ako 16.1R7-S8
Juniper Networks Junos OS vo verzii staršej ako 17.2R3-S4
Juniper Networks Junos OS vo verzii staršej ako 17.3R3-S8
Juniper Networks Junos OS vo verzii staršej ako 17.4R3-S2
Juniper Networks Junos OS vo verzii staršej ako 18.1R3-S10
Juniper Networks Junos OS vo verzii staršej ako 18.2R3-S3
Juniper Networks Junos OS vo verzii staršej ako 18.3R3-S2
Juniper Networks Junos OS vo verzii staršej ako 18.4R3-S2
Juniper Networks Junos OS vo verzii staršej ako 19.1R3
Juniper Networks Junos OS vo verzii staršej ako 19.2R2
Juniper Networks Junos OS vo verzii staršej ako 19.3R3
Juniper Networks Junos OS vo verzii staršej ako 19.4R2

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11105&cat=SIRT_1&actp=LIST

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 6.5
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Hitachi ABB Power Grids série AFS - bezpečnostná zraniteľnosť

Popis

Spoločnosť Hitachi vydala bezpečnostné aktualizácie na produkty ABB Power Grids, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje neautentifikovanému útočníkovi, ktorý sa nachádza v rovnakom sieťovom segmente, prostredníctvom zasielania špeciálne upravených HSR rámcov spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

16.03.2021

CVE

CVE-2020-9307

Zasiahnuté systémy

Hitachi ABB Power Grids AFS660 s firmware vo verzii staršej ako 7.1.03
Hitachi ABB Power Grids AFS665 s firmware vo verzii staršej ako 7.1.03

Následky

Zneprístupnenie služby

Odporúčania

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

Zdroje

https://us-cert.cisa.gov/ics/advisories/icsa-21-075-03
https://search.abb.com/library/Download.aspx?DocumentID=9AKK107991A9269&LanguageCode=en&DocumentPartId=&Action=Launch