BEZPEČNOSTNÝ BULLETIN

Týždeň 20. 07. 2022 - 26. 07. 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-838

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

Identifikátor

Apple - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Apple vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej požiadavky vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému. Na uvedenú zraniteľnosť je v súčasnosti verejne dostupný Proof-of-Concept kód.

Dátum prvého zverejnenia varovania

20.07.2022

CVE

CVE-2021-28544, CVE-2021-4136, CVE-2021-4166, CVE-2021-4173, CVE-2021-4187, CVE-2021-4192, CVE-2021-4193, CVE-2021-46059, CVE-2022-0128, CVE-2022-0156, CVE-2022-0158, CVE-2022-2294, CVE-2022-24070, CVE-2022-26704, CVE-2022-26768, CVE-2022-26981, CVE-2022-29046, CVE-2022-29048, CVE-2022-32781, CVE-2022-32784, CVE-2022-32785, CVE-2022-32786, CVE-2022-32787, CVE-2022-32788, CVE-2022-32789, CVE-2022-32792, CVE-2022-32793, CVE-2022-32796, CVE-2022-32797, CVE-2022-32798, CVE-2022-32799, CVE-2022-32800, CVE-2022-32801, CVE-2022-32802, CVE-2022-32805, CVE-2022-32807, CVE-2022-32810, CVE-2022-32811, CVE-2022-32812, CVE-2022-32813, CVE-2022-32814, CVE-2022-32815, CVE-2022-32816, CVE-2022-32817, CVE-2022-32818, CVE-2022-32819, CVE-2022-32820, CVE-2022-32821, CVE-2022-32823, CVE-2022-32824, CVE-2022-32825, CVE-2022-32826, CVE-2022-32828, CVE-2022-32829, CVE-2022-32830, CVE-2022-32831, CVE-2022-32832, CVE-2022-32834, CVE-2022-32837, CVE-2022-32838, CVE-2022-32839, CVE-2022-32840, CVE-2022-32841, CVE-2022-32842, CVE-2022-32843, CVE-2022-32844, CVE-2022-32845, CVE-2022-32847, CVE-2022-32848, CVE-2022-32849, CVE-2022-32851, CVE-2022-32852, CVE-2022-32853, CVE-2022-32855, CVE-2022-32857

Zasiahnuté systémy

Safari vo verzii staršej ako 15.6
watchOS verzii staršej ako 8.7
macOS Big Sur verzii staršej ako 11.6.8
macOS Monterey verzii staršej ako 12.5
tvOS verzii staršej ako 15.6
iOS verzii staršej ako 15.6
iPadOS verzii staršej ako 15.6

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.

Zdroje
https://support.apple.com/en-us/HT201222 https://github.com/Muirey03/CVE-2022-32832

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

Identifikátor

Google Chrome - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Google vydala bezpečnostnú aktualizáciu na svoj internetový prehliadač Chrome, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorenej webovej stránky vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

20.07.2022

CVE

CVE-2022-2163, CVE-2022-2477, CVE-2022-2478, CVE-2022-2479, CVE-2022-2480, CVE-2022-2481

Zasiahnuté systémy

Google Chrome vo verzii staršej ako 103.0.5060.134

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Rovnako odporúčame poučiť používateľov, aby neotvárali webové stránky a prílohy z neoverených zdrojov.
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/231487
https://chromereleases.googleblog.com/2022/07/stable-channel-update-for-desktop_19.html

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

Identifikátor

Rockwell Automation ISaGRAF Workbench - tri bezpečnostné zraniteľnosti

Popis

Spoločnosť Rockwell Automation vydala bezpečnostnú aktualizáciu na svoje softvérové dizajnérske prostredie ISaGRAF Workbench, ktorá opravuje tri bezpečnostné zraniteľnosti.
Bezpečnostné zraniteľnosti spočívajú v nedostatočnej implementácii bezpečnostných mechanizmov a umožňujú lokálnemu, neautentifikovanému útočníkovi prostredníctvom podrvhnutia špeciálne vytvorených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

21.07.2022

CVE

CVE-2022-2463, CVE-2022-2464, CVE-2022-2465

Zasiahnuté systémy

ISaGRAF Workbench vo verziách 6.0 až 6.6.9

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.

Zdroje

https://www.cisa.gov/uscert/ics/advisories/icsa-22-202-03

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

Identifikátor

Atlassian Confluence - tri bezpečnostné zraniteľnosti

Popis

Spoločnosť Atlassian vydala bezpečnostnú aktualizáciu na svoj produkt Confluence Server and Data Center, ktorá opravuje tri bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v existencii zabudovaného používateľského účtu s predvoleným heslom a umožňuje vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup do systému a následne úplnú kontrolu nad systémom.
Zraniteľnosť je v súčasnosti aktívne zneužívaná útočníkmi.

Dátum prvého zverejnenia varovania

20.07.2022

CVE

CVE-2022-26136, CVE-2022-26137, CVE-2022-26138

Zasiahnuté systémy

Confluence Server and Data Center vo verzii staršej ako 7.14.3, 7.15.2, 7.13.6, 7.16.4, 7.4.17, a 7.17.2

Následky

Neoprávnený prístup do systému
Úplné narušenie dôvernosti, integrity a dostupnosti systému

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.

Zdroje

https://jira.atlassian.com/browse/CONFSERVER-79483
https://confluence.atlassian.com/doc/confluence-security-advisory-2022-07-20-1142446709.html
https://securityonline.info/cve-2022-26138-hard-coded-password-confluence-server-and-data-center/

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

Identifikátor

ABB zariadenia s Totalflow protokolom - bezpečnostná zraniteľnosť

Popis

Spoločnosť ABB vydala bezpečnostné aktualizácie na svoje zariadenia využívajúce Totalflow TCP protokol, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť 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

14.07.2022

CVE

CVE-2022-0902

Zasiahnuté systémy

RMC-100 (Standard) vo verzii staršej ako 2105457-037
RMC-100-LITE vo verzii staršej ako 2106229-011
XIO vo verzii staršej ako 2106198-008
XFCG5 vo verzii staršej ako 2105805-016
XRCG5 vo verzii staršej ako 2105864-016
uFLOG5 vo verzii staršej ako 2105298-024
UDC vo verzii staršej ako 2106177-007

Následky

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

Odporúčania

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

Zdroje

https://search.abb.com/library/Download.aspx?DocumentID=9AKK108467A0927&LanguageCode=en&DocumentPartId=&Action=Launch

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

Identifikátor

Linux Kernel - bezpečnostná zraniteľnosť

Popis

Vývojári jadra operačného systému Linux vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť v spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa eskalovať svoje privilégiá a následne spôsobiť úplné narušenie dôvernosti, integrity a dostupnosti systému.
Na zraniteľnosť je v súčasnosti verejne dostupný Proof-of-Concept kód.

Dátum prvého zverejnenia varovania

20.07.2022

CVE

CVE-2022-34918

Zasiahnuté systémy

Linux kernel vo verzii staršej ako v5.19-rc7

Následky

Eskalácia privilégií
Úplné narušenie dôvernosti, integrity a dostupnosti systému.

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.

Zdroje

https://nvd.nist.gov/vuln/detail/CVE-2022-34918
https://randorisec.fr/crack-linux-firewall/
https://github.com/randorisec/CVE-2022-34918-LPE-PoC

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

Identifikátor

Zyxel - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť Zyxel vydala bezpečnostnú aktualizáciu na svoje portfólio produktov, ktorá opravuje dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zaslania špeciálne vytvorenej požiadavky spôsobiť úplné narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

19.07.2022

CVE

CVE-2022-2030, CVE-2022-30526

Zasiahnuté systémy

USG FLEX 100(W), 200, 500, 700 vo verzii staršej ako ZLD V5.31
USG FLEX 50(W) / USG20(W)-VPN vo verzii staršej ako ZLD V5.31
ATP series vo verzii staršej ako ZLD V5.31
VPN Series vo verzii staršej ako ZLD V5.31
USG/ZyWALL vo verzii staršej ako ZLD V4.72

Následky

Úplné narušenie dôvernosti, integrity a dostupnosti systému.

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.

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/231515
https://www.zyxel.com/support/Zyxel-security-advisory-authenticated-directory-traversal-vulnerabilities-of-firewalls.shtml

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

Identifikátor

Apache Skywalking NodeJS Agent - bezpečnostná zraniteľnosť

Popis

Spoločnosť Apache vydala bezpečnostnú aktualizáciu na svoj produkt Apache Skywalking NodeJS Agent, ktorá opravuje bezpečnostnú zraniteľnosť.
Zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej požiadavky spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

18.07.2022

CVE

CVE-2022-36127

Zasiahnuté systémy

Apache Skywalking NodeJS agent vo verzii staršej ako 0.5.1

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/231408

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.1**
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Grafana - bezpečnostná zraniteľnosť

Popis

Vývojári nástroja Grafana vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Predmetná zraniteľnosť spočíva v nedostatočnej implementácii mechanizmov autentifikácie a umožňuje vzdialenému, autentifikovanému útočníkovi získať úplnú kontrolu nad inými používateľskými účtami na danej inštancii Grafana.

Dátum prvého zverejnenia varovania

14.07.2022

CVE

CVE-2022-31107

Zasiahnuté systémy

Grafana vo verzii staršej ako 9.0.3, 8.5.9, 8.4.10, a 8.3.10

Následky

Neoprávnený prístup k citlivým údajom
Narušenie dôvernosti, integrity a dostupnosti systému.

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.

Zdroje

https://github.com/grafana/grafana/security/advisories/GHSA-mx47-6497-3fv2

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 6.3
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Drupal - viacero bezpečnostných zraniteľností

Popis

Vývojári redakčného systému Drupal vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami administrátora prostredníctvom podvrhnutia špeciálne vytvoreného súboru vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.
Ostatné zraniteľnosti by útočník mohol zneužiť na získanie neoprávneného prístupu k citlivým údajom.

Dátum prvého zverejnenia varovania

20.07.2022

CVE

CVE-2022-25275, CVE-2022-25276, CVE-2022-25277, CVE-2022-25278

Zasiahnuté systémy

Drupal vo verzii staršej ako 9.4.3.
Drupal vo verzii staršej ako 9.3.19.
Drupal vo verzii staršej ako 8 (vrátane)
poznámka: Drupal vo verzii 7 nie je zasiahnutý

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Rovnako odporúčame poučiť používateľov, aby neotvárali odkazy a prílohy z neoverených zdrojov.
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.cybersecurity-help.cz/vdb/SB2022072109
https://www.drupal.org/sa-core-2022-014