BEZPEČNOSTNÝ BULLETIN

Týždeň 14. 12. 2022 - 20. 12. 2022

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Aruba Orchestrator - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
02.	Apple - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
03.	Mozilla Firefox, ESR a Thunderbird - viacero bezpečnostných zraniteľností.	Vysoká	**8.8**
04.	Google Chrome - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
05.	Microsoft - viacero bezpečnostných zraniteľností	Vysoká	**8.5**
06.	Samba - viacero bezpečnostných zraniteľností	Vysoká	**8.1**
07.	VMware - dve bezpečnostné zraniteľnosti	Vysoká	**7.2**

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-969

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

Identifikátor

Aruba Orchestrator - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Aruba vydala bezpečnostné aktualizácie na svoje portfólio produktov Orchestrator, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom SQL injekcie vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

13.12.2022

CVE

CVE-2022-43519, CVE-2022-43520, CVE-2022-43521, CVE-2022-43522, CVE-2022-43523, CVE-2022-43524, CVE-2022-43525, CVE-2022-43526, CVE-2022-43527, CVE-2022-43528, CVE-2022-43529, CVE-2022-44534, CVE-2022-44535

Zasiahnuté systémy

Orchestrator vo verzii staršej ako 9.2.2.40291
Orchestrator vo verzii staršej ako 9.1.5.40037
Aruba EdgeConnect Enterprise Orchestrator release 8.10.x vo všetkých verziách (EoL)
Aruba EdgeConnect Enterprise Orchestrator release 9.0.x vo všetkých verziách (EoL)

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.
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.
V prípade, že aktualizácia systému nie je možná, pre minimalizáciu pravdepodobnosti zneužitia zraniteľností útočníkom výrobca odporúča obmedziť CLI a webové ovládacie rozhrania na dedikovaný segment/VLAN úrovne 2 alebo/a filtrovať sieťovú komunikáciu bezpečnostnými prvkami sieťovej infraštruktúry na úrovni 3 a vyššie.
Pri produktoch ktoré už nie sú udržiavané odporúčame prejsť na iný produkt s platnou podporou.

Zdroje

https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-021.txt

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 podvrhnutia špeciálne vytvorenej webovej stránky vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

13.12.2022

CVE

CVE-2022-24836, CVE-2022-29181, CVE-2022-32942, CVE-2022-32943, CVE-2022-40303, CVE-2022-40304, CVE-2022-42821, CVE-2022-42837, CVE-2022-42840, CVE-2022-42841, CVE-2022-42842, CVE-2022-42843, CVE-2022-42845, CVE-2022-42847, CVE-2022-42848, CVE-2022-42849, CVE-2022-42851, CVE-2022-42852, CVE-2022-42853, CVE-2022-42854, CVE-2022-42855, CVE-2022-42856, CVE-2022-42859, CVE-2022-42861, CVE-2022-42862, CVE-2022-42863, CVE-2022-42864, CVE-2022-42865, CVE-2022-42866, CVE-2022-42867, CVE-2022-46689, CVE-2022-46690, CVE-2022-46691, CVE-2022-46692, CVE-2022-46693, CVE-2022-46694, CVE-2022-46695, CVE-2022-46696, CVE-2022-46697, CVE-2022-46698, CVE-2022-46699, CVE-2022-46700, CVE-2022-46701

Zasiahnuté systémy

iCloud for Windows vo verzii staršej ako 14.1
macOS Ventura vo verzii staršej ako 13.1
macOS Monterey vo verzii staršej ako 12.6.2
macOS Big Sur vo verzii staršej ako 11.7.2
tvOS vo verzii staršej ako 16.2
watchOS vo verzii staršej ako 9.2
iOS vo verzii staršej ako 16.2
iPadOS vo verzii staršej ako 16.2
Safari vo verzii staršej ako 16.2

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://support.apple.com/en-us/HT201222 https://thehackernews.com/2022/12/new-actively-exploited-zero-day.html https://support.apple.com/en-us/HT213538 https://support.apple.com/en-us/HT213532 https://support.apple.com/en-us/HT213537 https://support.apple.com/en-us/HT213533 https://support.apple.com/en-us/HT213534 https://support.apple.com/en-us/HT213535 https://support.apple.com/en-us/HT213536 https://support.apple.com/en-us/HT213531 https://support.apple.com/en-us/HT213530 https://access.redhat.com/security/cve/cve-2022-42856

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

Identifikátor

Mozilla Firefox, ESR a Thunderbird - viacero bezpečnostných zraniteľností.

Popis

Spoločnosť Mozilla Foundation vydala bezpečnostné aktualizácie na produkty Mozilla Firefox, Firefox ESR a Thunderbird ktoré opravujú 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

13.12.2022

CVE

CVE-2022-46871, CVE-2022-46872, CVE-2022-46873, CVE-2022-46874, CVE-2022-46875, CVE-2022-46877, CVE-2022-46878, CVE-2022-46879, CVE-2022-46880, CVE-2022-46881, CVE-2022-46882

Zasiahnuté systémy

Thunderbird vo verzii staršej ako 102.6
Firefox vo verzii staršej ako 108
Firefox vo verzii staršej ako ESR 102.6

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.mozilla.org/en-US/security/advisories/mfsa2022-51/
https://www.mozilla.org/en-US/security/advisories/mfsa2022-52/
https://www.mozilla.org/en-US/security/advisories/mfsa2022-53/

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 Google 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

13.12.2022

CVE

CVE-2022-4436, CVE-2022-4437, CVE-2022-4438, CVE-2022-4439, CVE-2022-4440

Zasiahnuté systémy

Chrome vo verzii staršej ako 108.0.5359.124

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://chromereleases.googleblog.com/2022/12/stable-channel-update-for-desktop_13.html
https://nvd.nist.gov/vuln/detail/CVE-2022-4436

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 8.5
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Microsoft - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Microsoft vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností.

Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zneužitia bližšie nepopísanej zraniteľnosti vo frameworku PowerShell vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

13.12.2022

CVE

CVE-2022-24480, CVE-2022-26804, CVE-2022-26805, CVE-2022-26806, CVE-2022-41074, CVE-2022-41076, CVE-2022-41077, CVE-2022-41094, CVE-2022-41115, CVE-2022-41121, CVE-2022-41127, CVE-2022-4174, CVE-2022-4175, CVE-2022-4177, CVE-2022-4178, CVE-2022-4179, CVE-2022-4180, CVE-2022-4181, CVE-2022-4182, CVE-2022-4183, CVE-2022-4184, CVE-2022-4185, CVE-2022-4186, CVE-2022-4187, CVE-2022-4188, CVE-2022-4189, CVE-2022-4190, CVE-2022-4191, CVE-2022-4192, CVE-2022-4193, CVE-2022-4194, CVE-2022-4195, CVE-2022-44666, CVE-2022-44667, CVE-2022-44668, CVE-2022-44669, CVE-2022-44670, CVE-2022-44671, CVE-2022-44673, CVE-2022-44674, CVE-2022-44675, CVE-2022-44676, CVE-2022-44677, CVE-2022-44678, CVE-2022-44679, CVE-2022-44680, CVE-2022-44681, CVE-2022-44682, CVE-2022-44683, CVE-2022-44687, CVE-2022-44688, CVE-2022-44689, CVE-2022-44690, CVE-2022-44691, CVE-2022-44692, CVE-2022-44693, CVE-2022-44694, CVE-2022-44695, CVE-2022-44696, CVE-2022-44697, CVE-2022-44698, CVE-2022-44699, CVE-2022-44702, CVE-2022-44704, CVE-2022-44708, CVE-2022-44710, CVE-2022-44713, CVE-2022-47212, CVE-2022-47213

Zasiahnuté systémy
.NET Framework Azure Client Server Run-time Subsystem (CSRSS) Microsoft Bluetooth Driver Microsoft Dynamics Microsoft Edge (Chromium-based) Microsoft Graphics Component Microsoft Office Microsoft Office OneNote Microsoft Office Outlook Microsoft Office SharePoint Microsoft Office Visio Microsoft Windows Codecs Library Role: Windows Hyper-V SysInternals Windows Certificates Windows Contacts Windows DirectX Windows Error Reporting Windows Fax Compose Form Windows HTTP Print Provider Windows Kernel Windows PowerShell Windows Print Spooler Components Windows Projected File System Windows Secure Socket Tunneling Protocol (SSTP) Windows SmartScreen Windows Subsystem for Linux Windows Terminal Presnú špecifikáciu jednotlivých zasiahnutých produktov nájdete na odkazoch v sekcii ZDROJE

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://msrc.microsoft.com/update-guide/releaseNote/2022-Dec https://nvd.nist.gov/vuln/detail/CVE-2022-41076

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

Identifikátor

Samba - viacero bezpečnostných zraniteľností

Popis

Vývojári balíka Samba vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne upravených paketov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

15.12.2022

CVE

CVE-2022-37966, CVE-2022-37967, CVE-2022-38023, CVE-2022-45141

Zasiahnuté systémy

Samba vo verzii staršej ako 4.17.4, 4.16.8 a 4.15.13

Následky

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

Odporúčania

Odporúčame uistiť sa, či Vaše aplikácie nevyužívajú frameworky, knižnice, pluginy, SDK alebo moduly v zraniteľnej verzii. V prípade, že áno, zabezpečte bezodkladnú aktualizáciu všetkých komponentov, od ktorých závisí vaša aplikácia, na aktuálne verzie bez známych bezpečnostných zraniteľností.
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.samba.org/samba/security/CVE-2022-38023.html
https://thehackernews.com/2022/12/samba-issues-security-updates-to-patch.html
https://sensorstechforum.com/cve-2022-38023-severe-samba-vulnerability/

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

Identifikátor

VMware - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť VMware vydala bezpečnostnú aktualizáciu na svoj produkt vRealize Operations, ktorá opravuje dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami administrátora eskalovať svoje privilégiá a následne získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

15.12.2022

CVE

CVE-2022-31707, CVE-2022-31708

Zasiahnuté systémy

VMware vRealize Operations (vROps) vo verzii staršej ako 8.10.1, KB90232

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.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.
Administrátorom odporúčame filtrovať sieťovú komunikáciu bezpečnostnými prvkami sieťovej infraštruktúry.
Ak je potrebný vzdialený prístup, použite virtuálnu súkromnú sieť (VPN).
Administrátorom odporúčame limitovať prístup k administratívnemu rozhraniu a jeho funkciám zavedením zoznamu pre riadenie prístupov (ACL).

Zdroje

https://www.vmware.com/security/advisories/VMSA-2022-0034.html

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-969