BEZPEČNOSTNÝ BULLETIN

Týždeň 19. 10. 2022 - 25. 10. 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-923

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

Identifikátor

Cisco produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Cisco vydala bezpečnostné aktualizácie na svoje produkty Meraki, ISE a TelePresence CE, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejsia bezpečnostná zraniteľnosť sa nachádza v produkte Meraki MX, spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

17.10.2022

CVE

CVE-2022-20776, CVE-2022-20811, CVE-2022-20822, CVE-2022-20933, CVE-2022-20953, CVE-2022-20954, CVE-2022-20955, CVE-2022-20959

Zasiahnuté systémy

Cisco Meraki MX od 16.2 vo verzii staršej ako 16.16.6
Cisco Meraki MX 17.x vo verzii staršej ako 17.10.1
Cisco ISE 3.1 vo verzii staršej ako 3.1P5 (Nov 2022)
Cisco ISE 3.21 vo verzii staršej ako 3.2P1 (Jan 2023)
Cisco ISE 2.41 (všetky verzie)
Cisco ISE 2.6 (všetky verzie)
Cisco ISE 2.7 vo verzii staršej ako 2.7P8 (Oct 2022)
Cisco ISE 3.0 vo verzii staršej ako 3.0P7 (Feb 2023)
Cisco ISE 3.1 vo verzii staršej ako 3.1P4
Cisco ISE 3.2 vo verzii staršej ako 3.2P1 (Jan 2023)
Cisco TelePresence CE 9 (všetky verzie)
Cisco TelePresence CE 10 vo verzii staršej ako 10.19.1

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať bezodkladnú aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť vykonanie škodlivého kódu 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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-vnESbgBf
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-path-trav-Dz5dpzyM
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-xss-twLnpy3M
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-trav-beFvCcyu

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

Identifikátor

Adobe Illustrator - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť Adobe vydala bezpečnostné aktualizácie na svoj produkty Illustrator 2022 a 2021, ktoré opravujú dve bezpečnostné zraniteľnosti.
Obe zraniteľnosti spočívajú v nedostatočnom overovaní používateľských vstupov a umožňujú lokálnemu, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených PCX a CDR súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

18.10.2022

CVE

CVE-2022-38435, CVE-2022-38436

Zasiahnuté systémy

Adobe Illustrator 2022 vo verzii staršeja ko 27.0
Adobe Illustrator 2021 vo verzii staršej ako 26.5.1

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 vykonanie škodlivého kódu 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://helpx.adobe.com/security/products/illustrator/apsb22-56.html
https://www.securityweek.com/adobe-illustrator-vulnerabilities-rated-critical-exploitation-not-easy

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

Identifikátor

Bentley Systems MicroStation Connect - 2 bezpečnostné zraniteľnosti

Popis

Spoločnosť Bentley Systems vydala bezpečnostnú aktualizáciu na svoj produkt MicroStation Connect, ktorá opravuje 2 bezpečnostné zraniteľnosti.
Obe bezpečnostné zraniteľnosti spočívajú v nedostatočnom overovaní používateľských vstupov a umožňujú lokálnemu, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvoreného DGN súboru vykonať škodlivý kód s následkom úplného naruašenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

20.10.2022

CVE

CVE-2022-40201, CVE-2022-41613

Zasiahnuté systémy

Bentley Systems MicroStation Connect vo verzii staršej ako 17.1

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Riadiace systémy a jednotky odporúčame prevádzkovať úplne oddelené od internetu.
Po odstránení zraniteľností, ktoré mohli spôsobiť vykonanie škodlivého kódu 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://www.cisa.gov/uscert/ics/advisories/icsa-22-293-01

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

Identifikátor

Apple iOS a iPadOS - bezpečnostné zraniteľnosti

Popis

Spoločnosť Apple vydala bezpečnostné aktualizácie na svoje operačné systémy iOS a iPadOS, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť sa nachádza v kerneli oboch OS, spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorenej aplikácie vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.
Uvedená zraniteľnosť je v súčasnosti aktívne zneužívaná útočníkmi.

Dátum prvého zverejnenia varovania

24.10.2022

CVE

CVE-2022-22587, CVE-2022-22594, CVE-2022-22674, CVE-2022-22675, CVE-2022-32893, CVE-2022-32894, CVE-2022-32917, CVE-2022-42827

Zasiahnuté systémy

Apple iOS vo verzii staršej ako 16.1
Apple iPadOS vo verzii staršej ako 16

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame vykonať bezodkladnú aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť vykonanie škodlivého kódu 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.apple.com/en-us/HT213489
https://securityaffairs.co/wordpress/137579/security/apple-fixes-ninth-zero-day.html
https://www.bleepingcomputer.com/news/apple/apple-fixes-new-zero-day-used-in-attacks-against-iphones-ipads/

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

Identifikátor

Mozilla Firefox - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Mozilla vydala bezpečnostné aktualizácie na svoj internetový prehliadač Firefox, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejsia bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorenej URL adresy získať neoprávnený prístup k civlivým údajom.

Dátum prvého zverejnenia varovania

17.10.2022

CVE

CVE-2022-42927, CVE-2022-42928, CVE-2022-42929, CVE-2022-42930, CVE-2022-42931, CVE-2022-42932

Zasiahnuté systémy

Mozilla Firefox vo verzii staršej ako 106
Mozilla Firefox ESR vo verzii staršej ako 102.4

Následky

Neoprávnený prístup k civlivým údajom
Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť únik citlivých údajov 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://www.mozilla.org/en-US/security/advisories/mfsa2022-44/
https://www.mozilla.org/en-US/security/advisories/mfsa2022-45/
https://access.redhat.com/security/cve/cve-2022-42927

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

Identifikátor

F5 produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť F5 vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejsia bezpečnostná zraniteľnosť sa nachádza vo všetkých moduloch BIG-IP, spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

20.10.2022

CVE

CVE-2022-36795, CVE-2022-41617, CVE-2022-41624, CVE-2022-41691, CVE-2022-41694, CVE-2022-41741, CVE-2022-41742, CVE-2022-41743, CVE-2022-41770, CVE-2022-41780, CVE-2022-41787, CVE-2022-41806, CVE-2022-41813, CVE-2022-41832, CVE-2022-41833, CVE-2022-41835, CVE-2022-41836, CVE-2022-41983

Zasiahnuté systémy

BIG-IP
F5OS-A
F5OS-C
NGINX
BIG-IQ Centralized Management
Presný zoznam zasiahnutých verzií sa nachádza v odkaze v časti Zdroje.

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://support.f5.com/csp/article/K30425568

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.3**
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Avira Security pre Windows Nortonlifelock - bezpečnostná zraniteľnosť

Popis

Spoločnosť Nortonlifelock vydala bezpečnostnú aktualizáciu na svoj antivírus Avira Security pre Windows, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť vo funkcionalite slúžiacej na sťahovanie akualizácií spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi eskalovať svoje privilégiá a spôsobiť úplné narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

18.10.2021

CVE

CVE-2022-3368

Zasiahnuté systémy

Avira Security vo verzii staršej ako 1.1.72.30556

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://support.norton.com/sp/static/external/tools/security-advisories.html
https://nvd.nist.gov/vuln/detail/CVE-2022-3368