BEZPEČNOSTNÝ BULLETIN

Týždeň 10. 08. 2022 - 16. 08. 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-862

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

Identifikátor

Argo CD - viacero bezpečnostných zraniteľností

Popis

Vývojári GitOps nástroja pre Kubernetes Argo CD 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 vytvorených dát vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

19.05.2022

CVE

CVE-2021-23820, CVE-2022-2097, CVE-2022-28948, CVE-2022-30065

Zasiahnuté systémy

Argo CD vo verzii staršej ako 2.4.7

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://www.cybersecurity-help.cz/vdb/SB2022030706
https://www.securitynewspaper.com/2022/08/08/3-critical-vulnerabilities-in-argo-cd-allow-complete-take-over-of-your-applications-and-servers/
https://exchange.xforce.ibmcloud.com/vulnerabilities/212827

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

Identifikátor

Foxit PDF Reader a Editor - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Foxit vydala bezpečnostné aktualizácie na produkty Foxit PDF Reader a Foxit PDF Editor, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvoreného súboru alebo webovej stránky vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

29.07.2022

CVE

CVE-2022-37377

Zasiahnuté systémy

Foxit PDF Reader vo verzii staršej ako 12.0.1
Foxit PDF Editor vo verzii staršej ako 12.0.1

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 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.redpacketsecurity.com/foxit-pdf-reader-code-execution-cve-2022-37377/
https://www.zerodayinitiative.com/advisories/ZDI-22-1049/
https://www.foxit.com/support/security-bulletins.html

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

Identifikátor

Palo Alto Networks PAN-OS - bezpečnostná zraniteľnosť

Popis

Spoločnosť Palo Alto vydala bezpečnostnú aktualizáciu na platformu PAN-OS, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej požiadavky spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

10.08.2022

CVE

CVE-2022-0028

Zasiahnuté systémy

PAN-OS vo verzii staršej ako 10.2.2-h2
PAN-OS vo verzii staršej ako 10.1.6-h6
PAN-OS vo verzii staršej ako 10.0.11-h1
PAN-OS vo verzii staršej ako 9.1.14-h4
PAN-OS vo verzii staršej ako 9.0.16-h3
PAN-OS vo verzii staršej ako 8.1.23-h1

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://security.paloaltonetworks.com/CVE-2022-0028
https://exchange.xforce.ibmcloud.com/vulnerabilities/233220

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

Identifikátor

CISCO ASA a FTD - viacero bezpečnostných zraniteľností

Popis

Spoločnosť CISCO vydala bezpečnostné aktualizácie na produkty Adaptive Security Appliance a Firepower Threat Defense, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej požiadavky spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

10.08.2022

CVE

CVE-2021-1585, CVE-2022-20713, CVE-2022-20715, CVE-2022-20829, CVE-2022-20866

Zasiahnuté systémy

Cisco Adaptive Security Appliance (ASA) Software vo verzii staršej ako 9.8.4.44, 9.12.4.38, 9.14.4, 9.15.1.21, 9.16.2.14 a 9.17.1.7
Cisco Firepower Threat Defense (FTD) vo verzii staršej ako 6.4.0.15, 6.6.5.2, 7.0.2 a 7.1.0.1

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Cisco ASA Software vo verzii 9.7 a skorších ako aj 9.9, 9.10, a 9.13 už nie sú podporované, výrobca odporúča migrovať na podporovanú verziu.
Cisco FMC a FTD Software vo verzii 6.2.2 a skorších ako aj 6.3.0 a 6.5.0 už nie sú podporované, výrobca odporúča migrovať na podporovanú verziu.

Zdroje

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-dos-tL4uA4AA

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.3**
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Microsoft Edge (Chromium-based) - bezpečnostná zraniteľnosť

Popis

Spoločnosť Microsoft vydala bezpečnostnú aktualizáciu na svoj internetový prehliadač Edge, ktorá opravuje bezpečnostnú zraniteľnosť.
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

05.08.2022

CVE

CVE-2022-33636

Zasiahnuté systémy

Microsoft Edge (Chromium-based) vo verzii staršej ako 104.0.1293.47

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://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-33636
https://nvd.nist.gov/vuln/detail/CVE-2022-33636
https://www.redpacketsecurity.com/microsoft-edge-chromium-based-code-execution-cve-2022-33636/

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 8.2
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

SAP Business Intelligence Platform - bezpečnostná zraniteľnosť

Popis

Spoločnosť SAP vydala bezpečnostnú aktualizáciu na produkt Business Intelligence Platform, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup k citlivým údajom a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

09.08.2022

CVE

CVE-2022-32245

Zasiahnuté systémy

SAP BusinessObjects Business Intelligence Platform vo verzii staršej ako 420 a 430

Následky

Neoprávnený prístup k citlivým údajom
Zneprístupnenie služby

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://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html
https://launchpad.support.sap.com/
https://exchange.xforce.ibmcloud.com/vulnerabilities/233153

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

Identifikátor

Zimbra - bezpečnostná zraniteľnosť

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnosti e-mailového klienta Zimbra.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zasielania špeciálne vytvorených požiadaviek eskalovať svoje privilégiá a následne vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

10.08.2022

CVE

CVE-2022-37393

Zasiahnuté systémy

Zimbra vo verzii 8.8.15

Následky

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

Odporúčania

Na uvedenú zraniteľnosť v súčasnosti nebola vydaná bezpečnostná záplata, administrátorom preto odporúčame sledovať stránku výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.zimbra.com/
https://exchange.xforce.ibmcloud.com/vulnerabilities/233219