BEZPEČNOSTNÝ BULLETIN

Týždeň 16. 11. 2022 - 22. 11. 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-945

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

Identifikátor

f5 produkty - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť f5 vydala bezpečnostné aktualizácie na produkty iControl SOAP a iControl REST, ktoré opravujú dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorenej webovej stránky získať neoprávnený persistentný root prístup do systému a spôsobiť narušenie dôvernosti, integrity a dostupnosti systému.
Na zneužitie zraniteľnosti však musí podvrhnutú webstránku navštíviť administátor s aktívnou reláciou.

Dátum prvého zverejnenia varovania

16.11.2022

CVE

CVE-2022-41622, CVE-2022-41800

Zasiahnuté systémy

BIG-IP
BIG-IP SPK
BIG-IQ Centralized Management
Presnú špecifikáciu jednotlivých zasiahnutých produktov nájdete na odkazoch v sekcii ZDROJE

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.
Pri produktoch, pre ktoré ešte neboli vydané bezpečnostné záplaty, odporúčame zraniteľnosti mitigovať podľa odporúčaní od výrobcu, sledovať stránky výrobcu a po vydaní príslušných záplat systémy aktualizovať.

Zdroje

https://support.f5.com/csp/article/K94221585
https://support.f5.com/csp/article/K13325942
https://www.securityweek.com/remote-code-execution-vulnerabilities-found-f5-products

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

Identifikátor

Foxit Reader - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Foxit Software vydala bezpečnostnú aktualizáciu na svoj produkt Foxit Reader, 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 alebo PDF súboru vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

10.11.2022

CVE

CVE-2022-32774, CVE-2022-37332, CVE-2022-38097, CVE-2022-40129

Zasiahnuté systémy

Foxit Reader vo verzii staršej ako 12.0.1.12430

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://blog.talosintelligence.com/vulnerability-spotlight-use-after-free-vulnerabilities-in-foxit-reader-could-lead-to-arbitrary-code-execution/
https://www.foxit.com/support/security-bulletins.html

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

Identifikátor

Mozilla produkty - 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

15.11.2022

CVE

CVE-2022-40674, CVE-2022-45403, CVE-2022-45404, CVE-2022-45405, CVE-2022-45406, CVE-2022-45407, CVE-2022-45408, CVE-2022-45409, CVE-2022-45410, CVE-2022-45411, CVE-2022-45412, CVE-2022-45413, CVE-2022-45415, CVE-2022-45416, CVE-2022-45417, CVE-2022-45418, CVE-2022-45419, CVE-2022-45420, CVE-2022-45421

Zasiahnuté systémy

Mozilla Firefox vo verzii staršej ako 107
Firefox ESR vo verzii staršej ako 102.5
Thunderbird vo verzii staršej ako 102.5

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/mfsa2022-48/
https://www.mozilla.org/en-US/security/advisories/mfsa2022-47/
https://www.mozilla.org/en-US/security/advisories/mfsa2022-49/
https://exchange.xforce.ibmcloud.com/vulnerabilities/240142

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

Identifikátor

Zoom produkty - tri bezpečnostné zraniteľnosti

Popis

Spoločnosť Zoom vydala bezpečnostnú aktualizáciu na svoje portfólio produktov, ktorá opravuje tri bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa počas inštalačného procesu eskalovať svoje privilégiá, získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť znepristupnenie služby.

Dátum prvého zverejnenia varovania

15.11.2022

CVE

CVE-2022-28766, CVE-2022-28768, CVE-2022-36924

Zasiahnuté systémy

Zoom Rooms Installer pre Windows vo verzii staršej ako 5.12.6
Zoom Client for Meetings Installer pre macOS vo verzii staršej ako 5.12.6
Zoom Client for Meetings pre Windows (32-bit) vo verzii staršej ako 5.12.6
Zoom VDI Windows Meeting Client pre Windows (32-bit) vo verzii staršej ako 5.12.6
Zoom Rooms for Conference Room pre Windows (32-bit) vo verzii staršej ako 5.12.6

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://explore.zoom.us/en/trust/security/security-bulletin/

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

Identifikátor

HPE OfficeConnect & NetBatch-Plus - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť Hewlett Packard Enterprise vydala bezpečnostné aktualizácie na produkty OfficeConnect a NetBatch-Plus, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje neautentifikovanému útočníkovi, ktorý sa nachádza v rovnakom sieťovom segmente bližšie neopísanou metódou obísť autentifikáciu, získať neoprávnený prístup do systému, získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

17.11.2022

CVE

CVE-2022-37931, CVE-2022-37932

Zasiahnuté systémy

OfficeConnect 1820, 1850, a 1920S vo verzii staršej ako PT.02.14, PC.01.22, a PD.02.22
HPE NetBatch-Plus vo verzii staršej ako T9189L01^ABZ

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.
Manažmentové rozhrania zariadení a serverov odporúčame nesprístupňovať z verejného Internetu.

Zdroje

https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbnw04383en_us
https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbns04388en_us

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

Identifikátor

NetCloud OS - bezpečnostná zraniteľnosť

Popis

Spoločnosť Cradlepoint vydala bezpečnostnú aktualizáciu na svoj operačný systém NetCloud, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom injekcie špeciálne upravených príkazov vykonať škodlivý kód s následkom úplného antonovnarušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

17.11.2022

CVE

CVE-2022-3086

Zasiahnuté systémy

NetCloud OS vo verzii staršej ako v7.22.70

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 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.cisa.gov/uscert/ics/advisories/icsa-22-321-02

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

Identifikátor

Red Lion Crimson - bezpečnostná zraniteľnosť

Popis

Spoločnosť Red Lion Controls vydala bezpečnostné aktualizácie na svoje portfólio programovacieho softvéru Crimson, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom techniky path traversal získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

17.11.2022

CVE

CVE-2022-3090

Zasiahnuté systémy

Crimson 3.0 vo verzii staršej ako 711.00
Crimson 3.1 vo verzii staršej ako 3126.02
Crimson 3.2 vo verzii staršej ako 3.0045

Následky

Neoprávnený prístup k citlivým údajom

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.cisa.gov/uscert/ics/advisories/icsa-22-321-01

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

Identifikátor

ABB protection and control IED manager PCM600 - bezpečnostná zraniteľnosť

Popis

Spoločnosť ABB vydala bezpečnostnú aktualizáciu na svoj produkt ABB PCM600, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi prečítať prihlasovacie údaje používateľov zo súbora obsahujúceho zálohu a získať tak neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

15.11.2022

CVE

CVE-2022-2513

Zasiahnuté systémy

ABB PCM600 vo verzii staršej ako 2.11 + Hotfix 20220923

Následky

Neoprávnený prístup k citlivým údajom

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.
Pre dočasnú mitigáciu odporúčame postupovať podľa pokynov výrobcu uvedených na webovej adrese uvedenej v sekcii ZDROJE.

Zdroje

https://search.abb.com/library/Download.aspx?DocumentID=2NGA001518&LanguageCode=en&DocumentPartId=&Action=Launch&_ga=2.35280737.1553233210.1668756531-1784065056.1661159789

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

Identifikátor

Cisco ISE - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Cisco vydala bezpečnostné aktualizácie na svoj produkt Identity Services Engine, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zaslania špeciálne vytvorenej HTTP požiadavky získať neoprávnený prístup k citlivým údajom a vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

17.11.2022

CVE

CVE-2022-20956, CVE-2022-20959, CVE-2022-20964, CVE-2022-20965, CVE-2022-20966, CVE-2022-20967

Zasiahnuté systémy

Cisco Identity Services Engine 2.4 vo všetkých verziách
Cisco Identity Services Engine 2.6 vo všetkých verziách
Cisco Identity Services Engine 2.7 vo všetkých verziách
Cisco Identity Services Engine 3.0 vo všetkých verziách
Cisco Identity Services Engine 3.1 vo všetkých verziách
Cisco Identity Services Engine 3.2 vo všetkých verziách

Následky

Úplné narušenie dôvernosti a integrity systému.

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
V prípade, že aktualizácia systému nie je možná, odporúčame postupovať podľa pokynov výrobcu uvedených na odkazoch v sekcii ZDROJE.
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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-access-contol-EeufSUCx
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-7Q4TNYUx
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-xss-twLnpy3M

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.0**
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 spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom znovupoužitia uvoľnenej pamäte eskalovať svoje privilégiá a následne získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť znepristupnenie služby.

Dátum prvého zverejnenia varovania

14.11.2022

CVE

CVE-2022-3977

Zasiahnuté systémy

Linux Kernel
Presnú špecifikáciu jednotlivých zasiahnutých produktov nájdete na odkaze v sekcii ZDROJE

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://ubuntu.com/security/CVE-2022-3977
https://access.redhat.com/security/cve/CVE-2022-3977