BEZPEČNOSTNÝ BULLETIN

Týždeň 24. 08. 2022 - 30. 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-870

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

Identifikátor

Mozilla produkty - bezpečnostné zraniteľnosti

Popis

Spoločnosť Mozilla vydala bezpečnostné aktualizácie na produkty Firefox, Firefox ESR a Thunderbird, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť, nachádzajúca sa v internetovom prehliadači Mozilla Firefox, 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

14.04.2022

CVE

CVE-2022-38472, CVE-2022-38473, CVE-2022-38474, CVE-2022-38475, CVE-2022-38477, CVE-2022-38478

Zasiahnuté systémy

Mozilla Firefox 104
Mozilla Firefox ESR 91.13
Mozilla Firefox ESR 102.2
Mozilla Thunderbird 91.13
Mozilla Thunderbird 102.2

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 vykonanie škodlivého kódu a prístup 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.mozilla.org/en-US/security/advisories/mfsa2022-33/
https://www.mozilla.org/en-US/security/advisories/mfsa2022-34/
https://www.mozilla.org/en-US/security/advisories/mfsa2022-35/
https://www.mozilla.org/en-US/security/advisories/mfsa2022-36/

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

Identifikátor

Cisco produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Cisco vydala bezpečnostnú aktualizáciu na softwarové komponenty switchov ACI Multi-Site Orchestrator, FXOS, NX-OS a NX-OS Software OSPFv3, ktoré opravujú 4 bezpečnostné zraniteľnosti. Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa eskalovať svoje privilégiá a následne vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

25.08.2022

CVE

CVE-2022-20823, CVE-2022-20824, CVE-2022-20865, CVE-2022-20921

Zasiahnuté systémy
Cisco FXOS a NX-OS Firepower 4100 Series (CSCwb74498)
Cisco FXOS a NX-OS Firepower 9300 Security Appliances (CSCwb74498)
Cisco FXOS a NX-OS MDS 9000 Series Multilayer Switches (CSCwb74494)
Cisco FXOS a NX-OS Nexus 1000 Virtual Edge for VMware vSphere (CSCwb74495)
Cisco FXOS a NX-OS Nexus 1000V Switch for Microsoft Hyper-V (CSCwb74495)
Cisco FXOS a NX-OS Nexus 1000V Switch for VMware vSphere (CSCwb74495)
Cisco FXOS a NX-OS Nexus 3000 Series Switches (CSCwb70210)
Cisco FXOS a NX-OS Nexus 5500 Platform Switches (CSCwb74496)
Cisco FXOS a NX-OS Nexus 5600 Platform Switches (CSCwb74496)
Cisco FXOS a NX-OS Nexus 6000 Series Switches (CSCwb74496)
Cisco FXOS a NX-OS Nexus 7000 Series Switches (CSCwb74494)
Cisco FXOS a NX-OS Nexus 9000 Series Fabric Switches in ACI mode (CSCwb74493)
Cisco FXOS a NX-OS Nexus 9000 Series Switches in standalone NX-OS mode (CSCwb70210)
Cisco FXOS a NX-OS UCS 6200 Series Fabric Interconnects (CSCwb74497)
Cisco FXOS a NX-OS UCS 6300 Series Fabric Interconnects (CSCwb74497)
Cisco FXOS a NX-OS UCS 6400 Series Fabric Interconnects (CSCwb74513)
Cisco NX-OS Software OSPFv3 Nexus 3000 Series Switches (CSCvz68748)
Cisco NX-OS Software OSPFv3 Nexus 5500 Platform Switches (CSCwb50015)
Cisco NX-OS Software OSPFv3 Nexus 5600 Platform Switches (CSCwb50015)
Cisco NX-OS Software OSPFv3 Nexus 6000 Series Switches (CSCwb50015)
Cisco NX-OS Software OSPFv3 Nexus 7000 Series Switches (CSCwb50013)
Cisco NX-OS Software OSPFv3 Nexus 9000 Series Fabric Switches in ACI mode (CSCwb50012)
Cisco NX-OS Software OSPFv3 Nexus 9000 Series Switches in standalone NX-OS mode (CSCvz68748)
Cisco FXOS Firepower 1000 Series
Cisco FXOS Firepower 2100 Series
Cisco FXOS MDS 9000 Series Multilayer Switches
Cisco FXOS Nexus 1000 Virtual Edge for VMware vSphere
Cisco FXOS Nexus 1000V Switch for Microsoft Hyper-V
Cisco FXOS Nexus 1000V Switch for VMware vSphere
Cisco FXOS Nexus 3000 Series Switches
Cisco FXOS Nexus 5500 Platform Switches
Cisco FXOS Nexus 5600 Platform Switches
Cisco FXOS Nexus 6000 Series Switches
Cisco FXOS Nexus 7000 Series Switches
Cisco FXOS Nexus 9000 Series Fabric Switches in ACI mode
Cisco FXOS Nexus 9000 Series Switches in standalone NX-OS mode
Cisco FXOS UCS 6200 Series Fabric Interconnects
Cisco FXOS UCS 6300 Series Fabric Interconnects
Cisco FXOS UCS 6400 Series Fabric Interconnects
Cisco ACI Multi-Site Orchestrator vo verzii staršej ako 3.2

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

Odporúčania
Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov. V prípade zraniteľností FXOS a NX-OS, NX-OS Software OSPFv3 a FXOS administrátorom odporúčame postupovať podľa odporúčaní na stránkach výrobcu, ktoré môžete nájsť v časti Zdroje. 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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-mso-prvesc-BPFp9cZs https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cdp-dos-ce-wWvPucC9 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-ospfv3-dos-48qutcu https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fxos-cmdinj-TxcLNZNH

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

Identifikátor

Google Chrome - bezpečnostná zraniteľnosť

Popis

Spoločnosť Google vydala bezpečnostnú aktualizáciu na svoj webový prehliadač Google Chrome, ktorá opravuje bezpečnostnú zraniteľnosť.
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

30.08.2022

CVE

CVE-2022-3075

Zasiahnuté systémy

Google Chrome vo verzii staršej ako 105.0.5195.102

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://thehackernews.com/2022/09/google-release-urgent-chrome-update-to.html
https://www.tenable.com/plugins/nessus/164658
https://chromereleases.googleblog.com/2022/09/stable-channel-update-for-desktop.html

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

Identifikátor

Open-Xchange OX App Suite - bezpečnostná zraniteľnosť

Popis

Vývojári softwarového balíčka Open-Xchange vydala bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom injekcie špeciálne upravených príkazov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

03.09.2022

CVE

CVE-2022-29851

Zasiahnuté systémy

Open-Xchange vo verzii staršej ako 7.10.5-rev44, 7.10.6-rev16, 8.2.324

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.redpacketsecurity.com/open-xchange-ox-app-suite-code-execution-cve-2022-29851/
https://seclists.org/fulldisclosure/2022/Sep/0

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

Identifikátor

IBM MQ - bezpečnostné zraniteľnosti

Popis

Spoločnosť IBM vydala bezpečnostnú aktualizáciu na produkt MQ, ktorá opravuje 2 bezpečnostné zraniteľnosti v knižnici libcurl.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne vytvorených požiadaviek získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

22.08.2022

CVE

CVE-2022-27780, CVE-2022-30115

Zasiahnuté systémy

IBM MQ 9.1 LTS vo verzii staršej ako 9.1.0.11
IBM MQ 9.0 LTS vo verzii staršej ako 9.0.0.13
IBM MQ 9.2 CD vo verzii staršej ako 9.3.0
IBM MQ 9.1 CD vo verzii staršej ako 9.3.0
IBM MQ 9.2 LTS vo verzii staršej ako 9.2.0, Fix Pack 6 (9.2.0.6)

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť únik citlivých informácií, 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.ibm.com/support/pages/node/6614533