BEZPEČNOSTNÝ BULLETIN

Týždeň 27. 04. 2022 - 03. 05. 2022

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Johnson Controls Metasys ADS/ADX/OAS produkty - bezpečnostná zraniteľnosť	Vysoká	**8.8**
02.	Google Chrome - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
03.	Cisco ASA a FTD produkty - bezpečnostná zraniteľnosť	Vysoká	**8.6**
04.	Qt produkt - bezpečnostná zraniteľnosť	Vysoká	**7.8**
05.	Linuxové distribúcie na báze Debian - dve bezpečnostné zraniteľnosti 'Nimbuspwn'	Vysoká	**7.8**
06.	cURL nástroj - dve bezpečnostné zraniteľnosti	Vysoká	**7.5**

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-750

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

Identifikátor

Johnson Controls Metasys ADS/ADX/OAS produkty - bezpečnostná zraniteľnosť

Popis

Spoločnosť Johnson Controls vydala bezpečnostnú aktualizáciu na produkty Metasys ADS/ADX/OAS Servers, ktorá opravuje bezpečnostnú zraniteľnosť.
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

03.05.2022

CVE

CVE-2021-36207

Zasiahnuté systémy

Metasys ADS/ADX/OAS Servers vo verzii staršej ako 10.1.5
Metasys ADS/ADX/OAS Servers vo verzii staršej ako 11.0.2

Následky

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

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.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

https://us-cert.cisa.gov/ics/advisories/icsa-22-118-01

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 webového prehliadača Chrome, ktorá opravuje viacero bezpečnostných zraniteľností.

Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom povrhnutia špeciálne vytvorenej webovej stránky, vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

15.03.2022

CVE

CVE-2022-1477, CVE-2022-1478, CVE-2022-1479, CVE-2022-1481, CVE-2022-1482, CVE-2022-1483, CVE-2022-1484, CVE-2022-1485, CVE-2022-1486, CVE-2022-1487, CVE-2022-1488, CVE-2022-1489, CVE-2022-1490, CVE-2022-1491, CVE-2022-1492, CVE-2022-1493, CVE-2022-1494, CVE-2022-1495, CVE-2022-1496, CVE-2022-1497, CVE-2022-1498, CVE-2022-1499, CVE-2022-1500, CVE-2022-1501

Zasiahnuté systémy

Google Chrome vo verzii staršej ako 101.0.4951.41

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/2022/04/stable-channel-update-for-desktop_26.html

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

Identifikátor

Cisco ASA a FTD produkty - bezpečnostná zraniteľnosť

Popis

Spoločnosť Cisco vydala bezpečnostné aktualizácie na produkty Adaptive Security Appliance (ASA) a Firepower Threat Defense (FTD), ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

27.04.2022

CVE

CVE-2022-20715

Zasiahnuté systémy

Cisco ASA Software vo verzii staršej ako 9.15.1.21
Cisco ASA Software vo verzii staršej ako 9.16.2.14
Cisco ASA Software vo verzii staršej ako 9.17.1.7
Cisco FTD Software vo verzii staršej ako 6.4.0.15 (May 2022)
Cisco FTD Software vo verzii staršej ako 6.6.5.2
Cisco FTD Software vo verzii staršej ako 7.0.2 (May 2022)
Cisco FTD Software vo verzii staršej ako 7.1.0.1

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

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

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

Identifikátor

Qt produkt - bezpečnostná zraniteľnosť

Popis

Vývojári multiplatformovej knižnice Qt pre vytváranie programov s GUI 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 zasielania špeciálne vytvorenej požiadavky, eskalovať svoje privilégiá a následne vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

28.04.2022

CVE

CVE-2022-26873

Zasiahnuté systémy

Qt vo verzii staršej ako 5.14

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť lokálne 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.qt.io/
http://www.kb.cert.org/vuls/id/411271
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26873
https://exchange.xforce.ibmcloud.com/vulnerabilities/225372

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

Identifikátor

Linuxové distribúcie na báze Debian - dve bezpečnostné zraniteľnosti 'Nimbuspwn'

Popis

Bezpečnostní výskumníci zverejnili informácie o dvoch zraniteľnostiach Linuxového démona networkd-dispatcher.

Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa eskalovať svoje privilégiá a následne získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

27.04.2022

CVE

CVE-2022-29799, CVE-2022-29800

Zasiahnuté systémy

Linux Mint vo verzii staršej ako 20.3 (vrátane) s nainštalovaným networkd-dispatcher

Zraniteľné môžu byť aj ďalšie distribúcie Linuxu postavené na Debiane s nainštalovaným networkd-dispatcher

Následky

Eskalácia privilégií

Neoprávnený prístup k citlivým údajom

Neoprávnená zmena v systéme

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame sledovať stránku výrobcu a po vydaní bezpečnostných záplat 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.microsoft.com/security/blog/2022/04/26/microsoft-finds-new-elevation-of-privilege-linux-vulnerability-nimbuspwn/ https://thehackernews.com/2022/04/microsoft-discovers-new-privilege.html https://www.bleepingcomputer.com/news/security/new-nimbuspwn-linux-vulnerability-gives-hackers-root-privileges/ https://www.infosecurity-magazine.com/news/nimbuspwn-linux-bugs-could-provide/ https://gitlab.com/craftyguy/networkd-dispatcher/-/commit/074ff68f08d64a963a13e3cfc4fb3e3fb9006dfe https://www.helpnetsecurity.com/2022/04/27/cve-2022-29799-cve-2022-29800/

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

Identifikátor

cURL nástroj - dve bezpečnostné zraniteľnosti

Popis

Vývojári nástroja cURL vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne vytvorenej požiadavky, získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

27.04.2022

CVE

CVE-2022-27775, CVE-2022-27776

Zasiahnuté systémy

cURL vo verzii staršej ako 7.83.0

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://curl.se/docs/CVE-2022-27776.html
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-27776
https://exchange.xforce.ibmcloud.com/vulnerabilities/225296