BEZPEČNOSTNÝ BULLETIN

Týždeň 16. 02. 2022 - 22. 02. 2022

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Mozilla Thunderbird - bezpečnostná zraniteľnosť	Vysoká	**8.8**
02.	VMware produkty - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
03.	Google Chrome - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
04.	Apache Cassandra - bezpečnostná zraniteľnosť	Vysoká	**8.4**
05.	Docker Desktop - bezpečnostná zraniteľnosť	Vysoká	**7.8**
06.	Cisco ESA produkt - bezpečnostná zraniteľnosť	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-688

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

Identifikátor

Mozilla Thunderbird - bezpečnostná zraniteľnosť

Popis

Spoločnosť Mozilla vydala bezpečnostnú aktualizáciu na produkt Thunderbird, ktorá opravuje bezpečnostnú zraniteľnosť. Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

15.02.2022

CVE

CVE-2022-0566

Zasiahnuté systémy

Mozilla Thunderbird vo verzii staršej ako 91.6.0

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://www.mozilla.org/en-US/security/advisories/mfsa2022-07/
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0566
https://exchange.xforce.ibmcloud.com/vulnerabilities/219660
https://cyber.gc.ca/en/alerts/mozilla-security-advisory-av22-079

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

Identifikátor

VMware produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť VMware vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zasielania špeciálne vytvorenej požiadavky, vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

15.02.2022

CVE

CVE-2021-22040, CVE-2021-22041, CVE-2021-22042, CVE-2021-22043, CVE-2021-22050, CVE-2022-22945

Zasiahnuté systémy

VMware NSX Data Center pre vSphere vo verzii staršej ako 6.4.13
ESXi 7.0 U3 vo verzii staršej ako ESXi70U3c-19193900
ESXi 7.0 U2 vo verzii staršej ako ESXi70U2e-19290878
ESXi 7.0 U1 vo verzii staršej akoESXi70U1e-19324898
ESXi 6.7 vo verzii staršej ako ESXi670-202111101-SG
ESXi 6.5 vo verzii staršej ako ESXi650-202202401-SG
Fusion 12.x vo verzii staršej ako 12.2.1
Workstation 16.x vo verzii staršej ako 16.2.1

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.
Administrátorom odporúčame limitovať prístup k administratívnemu rozhraniu a jeho funkciám zavedením zoznamu pre riadenie prístupov (ACL).

Zdroje
https://www.vmware.com/security/advisories/VMSA-2022-0005.html
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22945
https://exchange.xforce.ibmcloud.com/vulnerabilities/219674
https://thehackernews.com/2022/02/vmware-issues-security-patches-for-high.html
https://www.auscert.org.au/bulletins/ESB-2022.0671
https://www.auscert.org.au/bulletins/ESB-2022.0672

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 na produkt 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

16.02.2022

CVE

CVE-2022-0099, CVE-2022-0308, CVE-2022-0453, CVE-2022-0456, CVE-2022-0460, CVE-2022-0465, CVE-2022-0603, CVE-2022-0608

Zasiahnuté systémy

Google Chrome vo verzii staršej ako 96.0.4664.194

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/2022/02/long-term-support-channel-update_16.html

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.4**
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Apache Cassandra - bezpečnostná zraniteľnosť

Popis

Združenie Apache vydalo bezpečnostnú aktualizáciu na svoj produkt Cassandra, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami administrátora vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

16.02.2022

CVE

CVE-2021-44521

Zasiahnuté systémy

Apache Cassandra vo verzii staršej ako 3.0.26
Apache Cassandra vo verzii staršej ako 3.11.12
Apache Cassandra vo verzii staršej ako 4.0.2

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://jfrog.com/blog/cve-2021-44521-exploiting-apache-cassandra-user-defined-functions-for-remote-code-execution/
https://thehackernews.com/2022/02/high-severity-rce-security-bug-reported.html
https://securityaffairs.co/wordpress/128079/breaking-news/apache-cassandra-rce.html?utm_source=rss&utm_medium=rss&utm_campaign=apache-cassandra-rce

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

Identifikátor

Docker Desktop - bezpečnostná zraniteľnosť

Popis

Vývojári nástroja Docker Desktop 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, získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť znepristupnenie služby.

Dátum prvého zverejnenia varovania

15.02.2022

CVE

CVE-2022-25365

Zasiahnuté systémy

Docker Desktop vo verzii staršej ako 4.5.1

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme
Znepristupnenie 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.
Administrátorom odporúčame limitovať prístup k administratívnemu rozhraniu a jeho funkciám zavedením zoznamu pre riadenie prístupov (ACL).

Zdroje

https://docs.docker.com/desktop/windows/release-notes/
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-25365
https://exchange.xforce.ibmcloud.com/vulnerabilities/220078

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

Identifikátor

Cisco ESA produkt - bezpečnostná zraniteľnosť

Popis

Spoločnosť Cisco vydala bezpečnostnú aktualizáciu na produkt Cisco Email Security Appliance (ESA), ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

16.02.2022

CVE

CVE-2022-20653

Zasiahnuté systémy

Cisco Email Security Appliance vo verzii staršej ako 13.0.3
Cisco Email Security Appliance vo verzii staršej ako 13.5.4.102
Cisco Email Security Appliance vo verzii staršej ako 14.0.2.020

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-dos-MxZvGtgU
https://thehackernews.com/2022/02/attackers-can-crash-cisco-email.html
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20653
https://exchange.xforce.ibmcloud.com/vulnerabilities/219777