BEZPEČNOSTNÝ BULLETIN

Týždeň 29. 04. 2020 - 05. 05. 2020

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Google Chrome viacero zraniteľností	Vysoká	**8.8**
02.	VMware ESXi zraniteľnosti	Vysoká	**8.4**
03.	Fortinet FortiMail a FortiVoiceEntreprise zraniteľnosť	Vysoká	**8.1**
04.	Cisco IOS XE SD-WAN zraniteľnosť	Vysoká	**7.8**
05.	Samba zraniteľnosť	Vysoká	**7.5**
06.	Cisco ASA chybný komponent	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:
01439/2020/SK-CERT-109

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

Identifikátor

Google Chrome viacero zraniteľností

Popis

Spoločnosť Google vydala aktualizáciu na svoj internetový prehliadač Google Chrome, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšie bezpečnostné zraniteľnosti umožňujú vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upraveného webového obsahu vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

27.04.2020

CVE

CVE-2020-6461, CVE-2020-6462

Zasiahnuté systémy

Google Chrome verzie staršie ako 81.0.4044.129

Následky

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

Odporúčania

Administrátorom 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://chromereleases.googleblog.com/2020/04/stable-channel-update-for-desktop_27.html
https://exchange.xforce.ibmcloud.com/vulnerabilities/180913
https://exchange.xforce.ibmcloud.com/vulnerabilities/180914

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

Identifikátor

VMware ESXi zraniteľnosti

Popis

Spoločnosť VMware vydala bezpečnostnú aktualizáciu na svoj produkt ESXi, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nedostatočným overovaním používateľských vstupov a umožňuje vzdialenému, autentifikovanému útočníkovi prostredníctvom XSS útoku vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

28.04.2020

CVE

CVE-2020-3955

Zasiahnuté systémy

VMware ESXi verzie staršie ako ESXi670-202004103-SG a ESXi650-201912104-SG

Následky

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

Odporúčania

Administrátorom zasiahnutých systémov odporúčame nainštalovať bezpečnostné aktualizácie.
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.vmware.com/security/advisories/VMSA-2020-0008.html
https://exchange.xforce.ibmcloud.com/vulnerabilities/180985

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.1**
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Fortinet FortiMail a FortiVoiceEntreprise zraniteľnosť

Popis

Spoločnosť Fortinet vydala aktualizáciu na svoje produkty FortiMail a FortiVoiceEntreprise, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov vo funkcii zmeny hesla a umožňuje vzdialenému, autentifikovanému útočníkovi získať neoprávnený prístup do systému.

Dátum prvého zverejnenia varovania

27.04.2020

CVE

CVE-2020-9294

Zasiahnuté systémy

FortiMail verzie staršie ako 5.4.11, 6.0.8 a 6.2.3
FortiVoiceEntreprise verzie staršie ako 6.0.2

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://fortiguard.com/psirt/FG-IR-20-045
https://exchange.xforce.ibmcloud.com/vulnerabilities/180852

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

Identifikátor

Cisco IOS XE SD-WAN zraniteľnosť

Popis

Spoločnosť Cisco vydala bezpečnostnú aktualizáciu na svoj produkt IOS XE SD-WAN, ktorá opravuje bezpečnostnú zraniteľnosť. Bezpečnostná zraniteľnosti je spôsobená nedostatočným overovaním používateľských vstupov v CLI komponente a umožňuje lokálnemu, autentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

29.04.2020

CVE

CVE-2019-16011

Zasiahnuté systémy

Cisco 1000 Series Aggregation Services Routers
Cisco 1000 Series Integrated Services Routers (ISRs)
Cisco 4000 Series ISRs
Cisco Cloud Services Router 1000V Series

Následky

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

Odporúčania

Administrátorom odporúčame bezodkladne 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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-xesdwcinj-AcQ5MxCn

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

Identifikátor

Samba zraniteľnosť

Popis

Vývojári produktu Samba vydali bezpečnostnú aktualizáciu, ktorá opravuje viacero bezpečnostných zraniteľností.
Bezpečnostné zraniteľnosti sú spôsobené nedostatočným overovaním používateľských vstupov v LDAP parseri a umožňujú vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne upravených paketov spôsobiť zneprístupnenie služieb.

Dátum prvého zverejnenia varovania

28.04.2020

CVE

CVE-2020-10700, CVE-2020-10704

Zasiahnuté systémy

Samba verzie staršie ako 4.10.15, 4.11.8 a 4.12.2

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov. Spojenie medzi Sambou a LDAP serverom odporúčame vždy chrániť prostredníctvom TLS. Návod môžete nájsť online napr. https://wiki.samba.org/index.php/Configuring_LDAP_over_SSL_(LDAPS)_on_a_Samba_AD_DC

Zdroje

https://www.samba.org/samba/security/CVE-2020-10704.html
https://www.samba.org/samba/security/CVE-2020-10700.html

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

Identifikátor

Cisco ASA chybný komponent

Popis

Spoločnosť Cisco informovala, že v jej produktoch ASA5508 a ASA5516 vyrobených medzi 18.05.2017 až 25.08.2017 sa môže nachádzať nevhodný rezistor. Po minimálne 18tich mesiacoch prevádzky môže dôjsť ku zlyhaniu daného komponentu, čím dôjde ku zneprístupneniu služieb.

Dátum prvého zverejnenia varovania

27.04.2020

CVE

-

Zasiahnuté systémy

Cisco ASA5508-FTD-K9
Cisco ASA5508-K9
Cisco ASA5508-K8
Cisco ASA5516-FPWR-K9
Cisco ASA5516-FTD-K9
Cisco ASA5516-FPWR-K8

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame overiť si možnú prítomnosť chybného komponentu zadaním sériového čísla zariadenia na https://snvui.cisco.com/snv/FN70476
V prípade pozitívneho výsledku odporúčame kontaktovať distribútora zariadenia.

Zdroje

https://www.cisco.com/c/en/us/support/docs/field-notices/704/fn70476.html