BEZPEČNOSTNÝ BULLETIN

Týždeň 08. 07. 2020 - 14. 07. 2020

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Citrix SD-WAN WANOP, ADC a Gateway - viacero zraniteľností	Vysoká	**8.8**
02.	Google Android - viacero zraniteľností	Vysoká	**8.8**
03.	VMware produkty - viacero zraniteľností	Vysoká	**7.8**
04.	Samba - zraniteľnosti	Vysoká	**7.5**
05.	Grundfos CIM 500 - 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:
01439/2020/SK-CERT-178

BEZPEČNOSTNÝ BULLETIN

Týždeň 08. 07. 2020 - 14. 07. 2020

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

Identifikátor

Citrix SD-WAN WANOP, ADC a Gateway - viacero zraniteľností

Popis

Spoločnosť Citrix vydala aktualizácie na svoje produkty Citrix SD-WAN WANOP, ADC a Gateway, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšie, bližšie nešpecifikované bezpečnostné zraniteľnosti, umožňujú vzdialenému neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

07.07.2020

CVE

CVE-2019-18177, CVE-2020-8187, CVE-2020-8190, CVE-2020-8191, CVE-2020-8193, CVE-2020-8194, CVE-2020-8195, CVE-2020-8196, CVE-2020-8197, CVE-2020-8198, CVE-2020-8199

Zasiahnuté systémy

Citrix Gateway Plug-in for Linux verzie staršie ako 1.0.0.137
Citrix SD-WAN WANOP verzie staršie ako 10.2.7, 11.0.3d a 11.1.1a
Citrix (NetScaler) ADC a Gateway verzie staršie ako 10.5-70.18, 11.1-64.14, 12.0-63.21, 12.1-57.18 a 13.0-58.30

Následky

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

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://support.citrix.com/article/CTX276688
https://www.citrix.com/blogs/2020/07/07/citrix-provides-context-on-security-bulletin-ctx276688/
https://us-cert.cisa.gov/ncas/current-activity/2020/07/08/citrix-releases-security-updates
https://www.theregister.com/2020/07/08/citrix_eleven_patches/
https://www.tenable.com/plugins/nessus/138212
https://thehackernews.com/2020/07/citrix-software-security-update.html

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

Identifikátor

Google Android - viacero zraniteľností

Popis

Spoločnosť Google vydala bezpečnostné aktualizácie na svoj operačný systém Android, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšie bezpečnostné zraniteľnosti umožňujú vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených súborov vykonať škodlivý kód v kontexte privilegovaného procesu s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

06.07.2020

CVE

CVE-2018-20669, CVE-2019-10580, CVE-2019-14123, CVE-2019-14124, CVE-2019-14130, CVE-2019-18282, CVE-2019-20636, CVE-2019-9501, CVE-2019-9502, CVE-2020-0107, CVE-2020-0122, CVE-2020-0224, CVE-2020-0225, CVE-2020-0226, CVE-2020-0227, CVE-2020-0228, CVE-2020-0230, CVE-2020-0231, CVE-2020-3688, CVE-2020-3698, CVE-2020-3699, CVE-2020-3700, CVE-2020-3701, CVE-2020-9589

Zasiahnuté systémy

Operačný systém Android so Security Patch Levels staršími ako 2020-07-05

Následky

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

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých systémov. Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov, nenavštevovali nedôveryhodné webové stránky a neinštalovali neoverené aplikácie.
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://source.android.com/security/bulletin/2020-07-01
https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-google-android-os-could-allow-for-arbitrary-code-execution_2020-091/

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

Identifikátor

VMware produkty - viacero zraniteľností

Popis

Spoločnosť VMware vydala bezpečnostné aktualizácie na svoje produkty VeloCloud Orchestrator, Fusion, Horizon a VMRC, ktoré opravujú bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť je spôsobená nedostatočným overovaním používateľských vstupov vo VeloCloud Orchestrator a umožňuje vzdialenému, autentifikovanému útočníkovi prostredníctvom SQL injection útoku získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

07.07.2020

CVE

CVE-2020-3973, CVE-2020-3974

Zasiahnuté systémy

VMware VeloCloud Orchestrator verzie staršie ako 3.4.1 a 3.3.2 p2
VMware VMRC for Mac verzie staršie ako 11.2.0
VMware Horizon Client for Mac verzie staršie ako 5.4.3
VMware Fusion verzie staršie ako 11.5.5

Následky

Neoprávnený prístup k citlivým údajom
Eskalácia privilégií

Odporúčania

Administrátorom zasiahnutých systémov odporúčame nainštalovať bezpečnostné aktualizácie.
Po odstránení zraniteľností, ktoré môžu spôsobiť únik informácií, 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.vmware.com/security/advisories/VMSA-2020-0017.html
https://www.vmware.com/security/advisories/VMSA-2020-0016.html
https://nvd.nist.gov/vuln/detail/CVE-2020-3973
https://nvd.nist.gov/vuln/detail/CVE-2020-3974

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

Identifikátor

Samba - zraniteľnosti

Popis

Vývojári produktu Samba vydali bezpečnostnú aktualizáciu, ktorá opravuje viacero bezpečnostných zraniteľností.
Bezpečnostné zraniteľnosti umožňujú vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne upravených paketov spôsobiť zneprístupnenie služieb.

Dátum prvého zverejnenia varovania

02.07.2020

CVE

CVE-2020-10700, CVE-2020-10730, CVE-2020-10745, CVE-2020-10760, CVE-2020-14303

Zasiahnuté systémy

Samba verzie staršie ako 4.10.17, 4.11.11 a 4.12.4

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.samba.org/samba/security/CVE-2020-10730.html
https://www.samba.org/samba/security/CVE-2020-14303.html
https://www.samba.org/samba/security/CVE-2020-10760.html
https://www.samba.org/samba/security/CVE-2020-10745.html

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

Identifikátor

Grundfos CIM 500 - zraniteľnosti

Popis

Spoločnosť Grundfos vydala aktualizácie pre svoje komunikačné moduly CIM 500, ktoré opravujú viacero bezpečnostných zraniteľností.
Bezpečnostné zraniteľnosti spočívajú v nedostatočnej implementácii bezpečnostných mechanizmov a umožňujú vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

07.07.2020

CVE

CVE-2020-10605, CVE-2020-10609

Zasiahnuté systémy

Grundfos CIM 500 verzie staršie ako 06.16.00

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré môžu spôsobiť únik informácií, je dobrou praxou 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-20-189-01