BEZPEČNOSTNÝ BULLETIN

Týždeň 22. 07. 2020 - 28. 07. 2020

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:
01439/2020/SK-CERT-186

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

Identifikátor

Adobe produkty - viacero zraniteľností

Popis

Spoločnosť Adobe vydala aktualizácie na portfólio svojich produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšie 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

21.07.2020

CVE

CVE-2020-9663, CVE-2020-9674, CVE-2020-9675, CVE-2020-9676, CVE-2020-9677, CVE-2020-9678, CVE-2020-9679, CVE-2020-9680, CVE-2020-9683, CVE-2020-9684, CVE-2020-9685, CVE-2020-9686, CVE-2020-9687

Zasiahnuté systémy

Adobe Bridge verzie staršie ako 10.1.1
Adobe Photoshop CC 2019 verzie staršie ako 20.0.10
Adobe Photoshop CC verzie staršie ako 21.2.1
Adobe Adobe Prelude verzie staršie ako 9.0.1
Adobe Reader Mobile verzie staršie ako 20.3

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému
Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom 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://helpx.adobe.com/security/products/bridge/apsb20-44.html https://helpx.adobe.com/security/products/photoshop/apsb20-45.html https://helpx.adobe.com/security/products/prelude/apsb20-46.html https://helpx.adobe.com/security/products/reader-mobile/apsb20-50.html https://www.theregister.com/2020/07/21/adobe_photoshop_patches/ https://threatpost.com/critical-adobe-photoshop-flaws-patched-in-emergency-update/157581/ https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-adobe-bridge-could-allow-for-arbitrary-code-execution-apsb20-44_2020-099/ https://exchange.xforce.ibmcloud.com/vulnerabilities/185614 https://exchange.xforce.ibmcloud.com/vulnerabilities/185613 https://exchange.xforce.ibmcloud.com/vulnerabilities/185611 https://exchange.xforce.ibmcloud.com/vulnerabilities/185607 https://exchange.xforce.ibmcloud.com/vulnerabilities/185610 https://exchange.xforce.ibmcloud.com/vulnerabilities/185612 https://exchange.xforce.ibmcloud.com/vulnerabilities/185609 https://exchange.xforce.ibmcloud.com/vulnerabilities/185608 https://exchange.xforce.ibmcloud.com/vulnerabilities/185603 https://exchange.xforce.ibmcloud.com/vulnerabilities/185604 https://exchange.xforce.ibmcloud.com/vulnerabilities/185606 https://exchange.xforce.ibmcloud.com/vulnerabilities/185602 https://exchange.xforce.ibmcloud.com/vulnerabilities/185601 https://www.zerodayinitiative.com/advisories/ZDI-20-911/ https://www.zerodayinitiative.com/advisories/ZDI-20-912/ https://www.zerodayinitiative.com/advisories/ZDI-20-913/ https://www.zerodayinitiative.com/advisories/ZDI-20-914/ https://www.zerodayinitiative.com/advisories/ZDI-20-915/ https://www.zerodayinitiative.com/advisories/ZDI-20-916/ https://www.zerodayinitiative.com/advisories/ZDI-20-917/ https://www.zerodayinitiative.com/advisories/ZDI-20-918/ https://www.zerodayinitiative.com/advisories/ZDI-20-919/ https://www.zerodayinitiative.com/advisories/ZDI-20-920/ https://www.zerodayinitiative.com/advisories/ZDI-20-921/ https://www.zerodayinitiative.com/advisories/ZDI-20-922/

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

Identifikátor

Citrix Workspace app - zraniteľnosť

Popis

Spoločnosť Citrix vydala aktualizáciu na svoj produkt Workspace app, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

21.07.2020

CVE

CVE-2020-8207

Zasiahnuté systémy

Citrix Workspace App for Windows verzie staršie ako 2006.1
Citrix Workspace App for Windows verzie staršie ako 1912 LTSR CU1

Následky

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

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/CTX277662
https://www.pentestpartners.com/security-blog/raining-system-shells-with-citrix-workspace-app/
https://www.securityweek.com/vulnerability-allows-remote-hacking-devices-running-citrix-workspace-app
https://securityaffairs.co/wordpress/106232/hacking/citrix-workspace-flaw.html
https://exchange.xforce.ibmcloud.com/vulnerabilities/185677

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 chýb a 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

27.07.2020

CVE

CVE-2020-6532, CVE-2020-6537, CVE-2020-6538, CVE-2020-6539, CVE-2020-6540, CVE-2020-6541

Zasiahnuté systémy

Google Chrome verzie staršie ako 84.0.4147.105

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/2020/07/stable-channel-update-for-desktop_27.html

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

Identifikátor

CODESYS V3 - zraniteľnosť

Popis

Spoločnosť CODESYS vydala bezpečnostnú aktualizáciu na portfólio svojich produktov CODESYS V3, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť vo funkcii CODESYSControlService.exe je spôsobená nedostatočným overovaním používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne upravených http požiadaviek spôsobiť pretečenie zásobníka a následne vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

23.07.2020

CVE

CVE-2020-15806

Zasiahnuté systémy

CODESYS V3 runtime systems verzie staršie ako 3.5.16.10

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

Zdroje

https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=13199&token=3e283c3e73fed61f7c181a7fa1169477efaf0c58&download=
https://www.tenable.com/security/research/tra-2020-46

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

Identifikátor

Phoenix Contact PLCnext Engineer - zraniteľnosť

Popis

Spoločnosť Phoenix Contact vydala bezpečnostnú aktualizáciu na svoj produkt PLCnext Engineer, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

21.07.2020

CVE

CVE-2020-12499

Zasiahnuté systémy

Phoenix Contact PLCnext Engineer verzie staršie ako 2020.6

Následky

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

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých systémov.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

https://cert.vde.com/en-us/advisories/vde-2020-025

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

Identifikátor

Cisco ASA a FTD - zraniteľnosť

Popis

Spoločnosť Cisco vydala bezpečnostné aktualizácie na svoje produkty ASA a FTD, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nedostatočným overovaním používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup k citlivým údajom. Zraniteľnosť je v súčasnosti aktívne zneužívaná útočníkmi.

Dátum prvého zverejnenia varovania

01.07.2020

CVE

CVE-2020-3452

Zasiahnuté systémy

Cisco Adaptive Security Appliance (ASA) verzie staršie ako 9.6.4.42, 9.8.4.20, 9.9.2.74, 9.10.1.42, 9.12.3.12, 9.13.1.10, 9.14.1.10
Cisco Firepower Threat Defense (FTD) verzie staršie ako 6.2.3.16, 6.4.0.9, 6.3.0.6, 6.4.0.10, 6.6.0.1, 6.5.0.5

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.

Zdroje

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-ro-path-KJuQhB86
https://exchange.xforce.ibmcloud.com/vulnerabilities/185682