BEZPEČNOSTNÝ BULLETIN

Týždeň 12. 06. 2019 - 18. 06. 2019

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Adobe Flash zraniteľnosť	Vysoká	**8.8**
02.	Google Chrome Blink zraniteľnosť	Vysoká	**8.8**
03.	Cisco IOS XE Software zraniteľnosť	Vysoká	**8.8**
04.	Schneider Electric ProClima zraniteľnosti	Vysoká	**7.8**
05.	Schneider Electric PowerSCADA Expert zraniteľnosť	Stredná	**6.5**
06.	Mozilla Thunderbird zraniteľnosti	Stredná	**6.5**

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:
01380/2019/TS/OKB-161

BEZPEČNOSTNÝ BULLETIN

Týždeň 12. 06. 2019 - 18. 06. 2019

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

Identifikátor

Adobe Flash zraniteľnosť

Popis

Spoločnosť Adobe vydala bezpečnostnú aktualizáciu na svoj produkt Flash, ktorá opravuje bezpečnostnú zraniteľnosť. Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upraveného súboru vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

11.06.2019

CVE

CVE-2019-7845

Zasiahnuté systémy

Adobe Flash Player Desktop Runtime verzie staršie ako 32.0.0.207
Adobe Flash Player for Google Chrome verzie staršie ako 32.0.0.207
Adobe Flash Player for Microsoft Edge and Internet Explorer 11 verzie staršie ako 32.0.0.207

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.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.

Zdroje

https://helpx.adobe.com/security/products/flash-player/apsb19-30.html
https://nvd.nist.gov/vuln/detail/CVE-2019-7845
https://www.cisecurity.org/advisory/a-vulnerability-in-adobe-flash-could-allow-for-arbitrary-code-execution-apsb19-30_2019-063/

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:
01380/2019/TS/OKB-161

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

Identifikátor

Google Chrome Blink zraniteľnosť

Popis

Spoločnosť Google vydala bezpečnostnú aktualizáciu na svoj produkt Chrome, ktorá opravuje bezpečnostnú zraniteľnosť v komponente Blink. Bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorenej webstránky vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

13.06.2019

CVE

CVE-2019-5842

Zasiahnuté systémy

Google Chrome verzie staršie ako 75.0.3770.90

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.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.

Zdroje

https://chromereleases.googleblog.com/2019/06/stable-channel-update-for-desktop_13.html
https://access.redhat.com/security/cve/cve-2019-5842

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

Identifikátor

Cisco IOS XE Software zraniteľnosť

Popis

Spoločnosť Cisco vydala bezpečnostnú aktualizáciu na svoj produkt IOS XE Software, ktorá opravuje bezpečnostné zraniteľnosti. Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorenej URL adresy vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

12.06.2019

CVE

CVE-2019-1904

Zasiahnuté systémy

Cisco IOS XE Software verzie s povolenou funkciou HTTP Server

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov. V prípade, že to nie je možné, odporúčame vypnutie funkcie HTTP Server.
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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190612-iosxe-csrf
https://linuxsecurity.com/advisories/red-hat/redhat-rhsa-2019-1477-01-important-chromium-browser-security-update?rss

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

Identifikátor

Schneider Electric ProClima zraniteľnosti

Popis

Spoločnosť Schneider Electric vydala bezpečnostnú aktualizáciu na svoj produkt ProClima, ktorá opravuje viacero bezpečnostných zraniteľností.
Bezpečnostné zraniteľnosti umožňujú lokálnemu útočníkovi, prostredníctvom podvrhnutia špeciálne upravených súborov, vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

11.06.2019

CVE

CVE-2019-6823, CVE-2019-6824, CVE-2019-6825

Zasiahnuté systémy

ProClima verzie staršie ako 8.0.0

Následky

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

Odporúčania

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

Zdroje

https://download.schneider-electric.com/files?p_enDocType=Technical+leaflet&p_File_Name=SEVD-2019-162-01-ProClima.pdf&p_Doc_Ref=SEVD-2019-162-01

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 6.5
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Schneider Electric PowerSCADA Expert zraniteľnosť

Popis

Spoločnosť Schneider Electric vydala bezpečnostnú aktualizáciu na svoj produkt PowerSCADA Expert, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť umožňuje lokálnemu, autentifikovanému útočníkovi získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

11.06.2019

CVE

CVE-2019-10981

Zasiahnuté systémy

PowerSCADA Expert 7.30
PowerSCADA Expert 7.40
PowerSCADA Expert 8.0 without Service Release 1

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

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

Zdroje

https://download.schneider-electric.com/files?p_enDocType=Technical+leaflet&p_File_Name=SEVD-2019-162-02-PowerSCADA-Expert.pdf&p_Doc_Ref=SEVD-2019-162-02

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 6.5
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Mozilla Thunderbird zraniteľnosti

Popis

Spoločnosť Mozilla vydala bezpečnostné aktualizácie na svoj mailový klient Thunderbird, ktoré opravujú viaceré bezpečnostné zraniteľnosti. Najvážnejšia bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorenej URL adresy spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

13.06.2019

CVE

CVE-2019-11703, CVE-2019-11704, CVE-2019-11705, CVE-2019-11706

Zasiahnuté systémy

Mozilla Thunderbird verzie staršie ako 60.7.1

Následky

Zneprístupnenie služby

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.

Zdroje

https://www.mozilla.org/en-US/security/advisories/mfsa2019-17/
https://exchange.xforce.ibmcloud.com/vulnerabilities/162605
https://exchange.xforce.ibmcloud.com/vulnerabilities/162606
https://exchange.xforce.ibmcloud.com/vulnerabilities/162607
https://exchange.xforce.ibmcloud.com/vulnerabilities/162608