BEZPEČNOSTNÝ BULLETIN

Týždeň 21. 03. 2018 – 27. 03. 2018

OBSAH BEZPEČNOSTNÉHO BULLETINU

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

Identifikátor

Mozilla Firefox Use-After-Free Vulnerability

Popis

Spoločnosť Mozilla vydala bezpečnostnú aktualizáciu, ktorá rieši bezpečnostnú zraniteľnosť v produktoch Firefox a Firefox ESR.
Zraniteľnosť by vzdialený neautentifikovaný útočník mohol prostredníctvom podvrhnutia škodlivého webového obsahu zneužiť na vykonanie škodlivého kódu a narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

26.03.2018

CVE

CVE-2018-5148

Zasiahnuté systémy

Mozilla Firefox verzie staršie ako 59.0.2
Mozilla Firefox ESR verzie staršie ako 52.7.3

Následky

Vykonanie škodlivého kódu a narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Administrátorom zasiahnutých systémov odporúčame bezodkladne nainštalovať bezpečnostné aktualizácie.

Zdroje

https://www.mozilla.org/en-US/security/advisories/mfsa2018-10/

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

Identifikátor

Dell EMC Isilon OneFS Multiple Vulnerabilities

Popis

Spoločnosť Dell vydala bezpečnostné aktualizácie na svoj produkt EMC Isilon OneFS, ktoré opravujú viacero bezpečnostných zraniteľností.
Najvážnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému autentifikovanému útočníkovi prostredníctvom CSRF (Cross-Site Request Forgery) útoku vykonať škodlivý kód.

Dátum prvého zverejnenia varovania

14.02.2018 (posledná aktualizácia 19.03.2018)

CVE

CVE-2018-1186, CVE-2018-1187, CVE-2018-1188, CVE-2018-1189, CVE-2018-1201, CVE-2018-1202, CVE-2018-1203, CVE-2018-1204, CVE-2018-1213

Zasiahnuté systémy

Dell EMC Isilon OneFS

Následky

Vykonanie škodlivého kódu

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých produktov.

Zdroje

http://seclists.org/fulldisclosure/2018/Mar/50
https://www.coresecurity.com/advisories/dell-emc-isilon-onefs-multiple-vulnerabilities

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

Identifikátor

F5 BIG-IP Multiple Vulnerabilities

Popis

Spoločnosť F5 vydala bezpečnostné aktualizácie na svoje produkty BIG-IP, ktoré opravujú viacero bezpečnostných zraniteľností.
Najvážnejšia bezpečnostná zraniteľnosť spočíva v nesprávnom spracovaní WebSocket paketov v komponente TMM (Traffic Management Microkernel) a vzdialený neautentifikovaný útočníkovi by ju prostredníctvom zasielania špeciálne upravených WebSocket paketov mohol zneužiť na vykonanie škodlivého kódu.

Dátum prvého zverejnenia varovania

21.03.2018

CVE

CVE-2018-5502, CVE-2018-5503, CVE-2018-5504, CVE-2018-5505, CVE-2018-5509

Zasiahnuté systémy

BIG-IP (ASM and Analytics) 13.1.0
BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, Edge Gateway, GTM, Link Controller, PEM, WebAccelerator, WebSafe) verzie 13.0.0 až 13.1.0 a 12.0.0 až 12.1.3

Následky

Vykonanie škodlivého kódu, Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých produktov.

Zdroje

https://support.f5.com/csp/article/K23520761
https://support.f5.com/csp/article/K54562183
https://support.f5.com/csp/article/K11718033
https://support.f5.com/csp/article/K43121447
https://support.f5.com/csp/article/K49440608

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

Identifikátor

Citrix XenServer Multiple Security Updates

Popis

Spoločnosť Citrix vydala bezpečnostné aktualizácie na svoje produkty XenServer, ktoré opravujú viacero bezpečnostných zraniteľností.
Najvážnejšia bezpečnostná zraniteľnosť umožňuje lokálnemu autentifikovanému útočníkovi spôsobiť zneprístupnenie služieb a eskalovať svoje privilégiá na napadnutom systéme.

Dátum prvého zverejnenia varovania

21.03.2018

CVE

CVE-2016-2074, CVE-2018-7540, CVE-2018-7541

Zasiahnuté systémy

Citrix XenServer verzie 7.0 až Citrix XenServer 7.3

Následky

Zneprístupnenie služby, Eskalácia privilégií

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých produktov.

Zdroje

https://support.citrix.com/article/CTX232655

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

Identifikátor

Netpbm Denial Of Service Vulnerability

Popis

Produkt Netpbm obsahuje bezpečnostnú zraniteľnosť, ktorú by vzdialený neautentifikovaný útočník mohol prostredníctvom podvrhnutia špeciálne vytvoreného súboru zneužiť na zneprístupnenie služieb. Zraniteľnosť sa nachádza vo funkcii *pm_mallcarray2* a spočíva v nedostatočnom overovaní používateľských vstupov.

Dátum prvého zverejnenia varovania

24.03.2018

CVE

CVE-2018-8975

Zasiahnuté systémy

Netpbm verzie 10.47.00, 10.47.01, 10.47.02, 10.47.03, 10.47.04, 10.47.05, 10.47.06, 10.81.03, 10.61.02

Následky

Zneprístupnenie služby

Odporúčania

Na uvedenú zraniteľnosť v súčasnosti nie sú dostupné aktualizácie. Používateľom zasiahnutých produktov odporúčame sledovať stránky výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu.

Zdroje

https://tools.cisco.com/security/center/viewAlert.x?alertId=57275
https://github.com/xiaoqx/pocs/tree/master/netpbm

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre: 5.3**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Omron CX-Supervisor Multiple Vulnerabilities

Popis

Spoločnosť Omron vydala bezpečnostnú aktualizáciu na svoj produkt CX-Supervisor, ktorá opravuje viacero bezpečnostných zraniteľností.
Bezpečnostné zraniteľnosti umožňujú lokálnemu neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených súborov spôsobiť pretečenie zásobníka a vykonať škodlivý kód.

Dátum prvého zverejnenia varovania

14.03.2018

CVE

CVE-2018-7513, CVE-2018-7515, CVE-2018-7517, CVE-2018-7519, CVE-2018-7521, CVE-2018-7523, CVE-2018-7525

Zasiahnuté systémy

CX-Supervisor verzia 3.30 a staršie

Následky

Vykonanie škodlivého kódu

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých produktov.

Zdroje

https://ics-cert.us-cert.gov/advisories/ICSA-18-072-01
https://www.myomron.com/index.php?action=kb&article=1707

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre: 5.3**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Denial-of-Service Vulnerability in Multiple Industrial Products

Popis

Spoločnosť Siemens vydala bezpečnostné aktualizácie na svoje produkty SIMATIC, SINUMERIK a Softnet PROFINET IO, ktoré opravujú spoločnosťou bližšie nešpecifikovanú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť umožňuje vzdialenému útočníkovi, ktorý disponuje priamym prístupom k zariadeniu na linkovej vrstve, prostredníctvom podvrhnutia špeciálne upravených PROFINET DCP paketov spôsobiť zneprístupnenie služieb.

Dátum prvého zverejnenia varovania

20.03.2018

CVE

CVE-2018-4843

Zasiahnuté systémy

SIMATIC CP 343, SIMATIC CP 443, SIMATIC S7, SINUMERIK 828D, SINUMERIK 840D, Softnet PROFINET IO

Následky

Zneprístupnenie služby

Odporúčania

Spoločnosť Siemens vydala aktualizácie na niektoré zo zraniteľných zariadení a ďalšie plánuje vydať v nasledujúcich dňoch. Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov, aplikovať firewallové pravidlá a limitovať prístup k zasiahnutým zariadeniam. Tiež odporúčame sledovať stránky výrobcu a po vydaní dodatočných bezpečnostných záplat vykonať aktualizáciu.

Zdroje

https://cert-portal.siemens.com/productcert/pdf/ssa-592007.pdf

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre: 5.3**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Apache HTTP Server Multiple Vulnerabilities

Popis

Spoločnosť Apache vydala bezpečnostnú aktualizáciu na svoj produkt Apache HTTP Server, ktorá opravuje viacero zraniteľností spočívajúcich v nesprávnej implementácii bezpečnostných mechanizmov.
Najzávažnejšiu zraniteľnosť vo funkcii *mod_session* by vzdialený autentifikovaný útočník mohol zneužiť na získanie prístupu k citlivým údajom.

Dátum prvého zverejnenia varovania

21.03.2018 (posledná aktualizácia 26.03.2018)

CVE

CVE-2017-15710, CVE-2017-15715, CVE-2018-1301, CVE-2018-1302, CVE-2018-1303, CVE-2018-1312, CVE-2018-1283

Zasiahnuté systémy

Apache HTTP Server pred verziou 2.4.30

Následky

Neoprávnený prístup k citlivým údajom, Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

http://httpd.apache.org/security/vulnerabilities_24.html#CVE-2018-1312
https://tools.cisco.com/security/center/viewAlert.x?alertId=57279