BEZPEČNOSTNÝ BULLETIN

Týždeň 25. 07. 2018 – 31. 07. 2018

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Google Stable Channel Update for Desktop July 2018	Vysoká	**8.8**
02.	WECON LeviStudioU Multiple Remote Code Execution Vulnerabilities	Vysoká	**8.8**
03.	Apache OpenWhisk Multiple Vulnerabilities	Vysoká	**8.8**
04.	GitLab Security Release: 11.1.2, 11.0.5, and 10.8.7	Vysoká	**8.8**
05.	XClarity Administrator (LXCA) API Vulnerabilities	Vysoká	**8.8**
06.	McAfee Web Gateway and Data Loss Prevention Endpoint Vulnerabilities	Vysoká	**7.5**
07.	F5 BIG-IP Multiple Vulnerabilities	Vysoká	**7.5**
08.	Apache Tomcat WebSocket Client Hostname Verification Bypass Vulnerability	Vysoká	**7.5**
09.	Dell EMC NetWorker Clear-Text Authentication Over Network Vulnerability	Stredná	**6.3**
10.	VMware Horizon View Agent, ESXi, Workstation and Fusion Multiple Vulnerabilities	Stredná	**5.5**

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:
02049/2018/TS/OKB-102

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

Identifikátor

Google Stable Channel Update for Desktop July 2018

Popis

Spoločnosť Google vydala bezpečnostnú aktualizáciu na svoj internetový prehliadač Chrome, verzia 68.0.3440.75, ktorá opravuje viacero chýb a bezpečnostných zraniteľností.
Najzávažnejšie sú bezpečnostné zraniteľnosti v komponentoch Skia, WebGl a WebRTC a vzdialený neautentifikovaný útočník by ich prostredníctvom podvrhnutia špeciálne vytvoreného webového obsahu mohol zneužiť na vykonanie škodlivého kódu v kontexte prehliadača.
Nová aktualizácia tiež v záujme zvýšenia bezpečnosti prehliadania označuje stránky, ktoré nevyužívajú zabezpečený protokol HTTPS, za nezabezpečené (Not secured).

Dátum prvého zverejnenia varovania

24.08.2018

CVE

CVE-2018-4117, CVE-2018-6044, CVE-2018-6153, CVE-2018-6154, CVE-2018-6155, CVE-2018-6156, CVE-2018-6157, CVE-2018-6158, CVE-2018-6159, CVE-2018-6160, CVE-2018-6161, CVE-2018-6162, CVE-2018-6163, CVE-2018-6164, CVE-2018-6165, CVE-2018-6166, CVE-2018-6167, CVE-2018-6168, CVE-2018-6169, CVE-2018-6170, CVE-2018-6171, CVE-2018-6172, CVE-2018-6173, CVE-2018-6174, CVE-2018-6175, CVE-2018-6176, CVE-2018-6177, CVE-2018-6178, CVE-2018-6179

Zasiahnuté systémy

Google Chrome verzie staršie ako 68.0.3440.75

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://chromereleases.googleblog.com/2018/07/stable-channel-update-for-desktop.html
https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-google-chrome-could-allow-for-arbitrary-code-execution_2018-084/

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

Identifikátor

WECON LeviStudioU Multiple Remote Code Execution Vulnerabilities

Popis

Bezpečnostní výskumníci zo Zero Day Initiative v spolupráci s ICS-CERT vydali bezpečnostné varovanie na 89 zero-day zraniteľností v produkte WECOM LeviStudioU slúžiacom na programovanie HMI (Human Machine Interface) rozhraní.
Bezpečnostné zraniteľnosti spočívajúce v nedostatočnom overovaní veľkosti dát pred kopírovaním do pamäte by vzdialený neautentifikovaný útočník prostredníctvom podrhnutia špeciálne vytvorených súborov mohol zneužiť na vyvolanie pretečenia zásobníka a následné vykonanie škodlivého kódu s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

26.07.2018

CVE

-

Zasiahnuté systémy

WECON LeviStudioU

Následky

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

Odporúčania

Na uvedené zraniteľnosti v súčasnosti nie sú dostupné aktualizácie. Administrátorom odporúčame poučiť používateľov, aby neotvárali prílohy a súbory z neznámych a neoverených zdrojov. Rovnako odporúčame sledovať stránku výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.zerodayinitiative.com/advisories/ZDI-18-784/
až
https://www.zerodayinitiative.com/advisories/ZDI-18-873/

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

Identifikátor

Apache OpenWhisk Multiple Vulnerabilities

Popis

Spoločnosť Apache vydala bezpečnostnú aktualizáciu na svoj produkt Apache OpenWhisk, ktorá opravuje viacero bezpečnostných zraniteľností.
Bezpečnostné zraniteľnosti v komponente PHP Runtime by vzdialený neautentifikovaný útočník mohol zneužiť na vykonanie škodlivého kódu a neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

23.07.2018

CVE

CVE-2018-11756, CVE-2018-11757

Zasiahnuté systémy

Apache OpenWhisk verzia 1.3.0 a staršie

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.puresec.io/hubfs/Apache%20OpenWhisk%20PureSec%20Security%20Advisory.pdf?t=1532417170859
https://nvd.nist.gov/vuln/detail/CVE-2018-11756
https://nvd.nist.gov/vuln/detail/CVE-2018-11757

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

Identifikátor

GitLab Security Release: 11.1.2, 11.0.5, and 10.8.7

Popis

Spoločnosť GitLab vydala bezpečnostné aktualizácie, ktoré opravujú viacero bezpečnostných zraniteľností v produkte GitLab Community and Enterprise Edition.
Najzávažnejšiu zraniteľnosť by vzdialený neautentifikovaný útočník mohol prostredníctvom CSRF (Cross-Site Request Forgery) útoku zneužiť na vykonanie príkazov v kontexte prihláseného používateľa.
Ďalšia skupina zraniteľností spočíva v nedostatočnom overovaní používateľských vstupov a vzdialený neautentifikovaný útočník by ju mohol zneužiť na realizáciu XSS (Cross-Site Scripting) útoku, vykonanie škodlivého kódu vo webovom prehliadači a získanie prístupu k údajom uloženým v cookies, vrátane autentifikačných údajov.
Ostatné zraniteľnosti by vzdialený neautentifikovaný útočník mohol zneužiť na zneprístupnenie služby a neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

26.07.2018

CVE

CVE-2018-14601, CVE-2018-14602, CVE-2018-14603, CVE-2018-14604, CVE-2018-14605, CVE-2018-14606

Zasiahnuté systémy

GitLab Community Edition (CE) and Enterprise Edition (EE) verzie staršie ako 11.1.2, 11.0.5, a 10.8.7

Následky

Vykonanie škodlivého kódu, Zneprístupnenie služby, Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://about.gitlab.com/2018/07/26/security-release-gitlab-11-dot-1-dot-2-released/

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

Identifikátor

XClarity Administrator (LXCA) API Vulnerabilities

Popis

Spoločnosť Lenovo vydala bezpečnostnú aktualizáciu na svoj produkt XClarity Administrator (LXCA), ktorá opravuje bezpečnostné zraniteľnosti vo web API.
Bližšie nešpecifikované bezpečnostné zraniteľnosti by vzdialený autentifikovaný útočník mohol zneužiť na neoprávnený prístup k citlivým údajom a eskaláciu privilégií na napadnutom systéme.

Dátum prvého zverejnenia varovania

26.07.2018

CVE

CVE-2018-9064, CVE-2018-9065, CVE-2018-9066

Zasiahnuté systémy

XClarity Administrator (LXCA) verzie staršie ako 2.1.0

Následky

Neoprávnený prístup k citlivým údajom, Eskalácia privilégií

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://support.lenovo.com/sk/en/solutions/len-22168

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.6**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

McAfee Web Gateway and Data Loss Prevention Endpoint Vulnerabilities

Popis

Spoločnosť McAfee vydala bezpečnostné aktualizácie, ktoré opravujú viaceré bezpečnostné zraniteľnosti v produktoch Web Gateway a Data Loss Prevention Endpoint.
Zraniteľnosti produkte Web Gateway spočívajú v nedostatočnej implementácii bezpečnostných mechanizmov v používateľskom rozhraní a vzdialený autentifikovaný útočník by ich mohol zneužiť na eskaláciu privilégií a vykonanie škodlivého kódu.
Zraniteľnosť v produkte Data Loss Prevention Endpoint spočíva v nedostatočnej implementácii mechanizmov riadenia prístupu a lokálny autentifikovaný útočník by ju mohol zneužiť na eskaláciu privilégií.

Dátum prvého zverejnenia varovania

16.07.2018 (posledná aktualizácia 24.07.2018)

CVE

CVE-2018-6677, CVE-2018-6678,CVE-2018-6683

Zasiahnuté systémy

McAfee Web Gateway verzie staršie ako 7.8.2
McAfee Data Loss Prevention Endpoint 11.0.x verzie staršie ako 11.0.405
McAfee Data Loss Prevention Endpoint 10.0.x verzie staršie ako 10.0.505

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://kc.mcafee.com/corporate/index?page=content&id=SB10245
https://kc.mcafee.com/corporate/index?page=content&id=SB10246

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

Identifikátor

F5 BIG-IP Multiple Vulnerabilities

Popis

Spoločnosť F5 vydala bezpečnostné aktualizácie na svoj produkt BIG-IP, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšie sú bližšie nešpecifikované bezpečnostné zraniteľnosti v komponente TMM (Traffic Management Microkernel) a BD procese a vzdialený neautentifikovaný útočník by ich mohol zneužiť na zneprístupnenie služby.

Dátum prvého zverejnenia varovania

19.07.2018 (posledná aktualizácia 24.07.2018)

CVE

CVE-2018-5530, CVE-2018-5531, CVE-2018-5536, CVE-2018-5537, CVE-2018-5538, CVE-2018-5539, CVE-2018-5540, CVE-2018-5541, CVE-2018-5542, CVE-2018-5533

Zasiahnuté systémy

BIG-IP

Následky

Zneprístupnenie služby, Neoprávnený prístup k citlivým údajom, Eskalácia privilégií

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://support.f5.com/csp/article/K45611803
https://support.f5.com/csp/article/K64721111
https://support.f5.com/csp/article/K27391542
https://support.f5.com/csp/article/K94105051
https://support.f5.com/csp/article/K45435121
https://support.f5.com/csp/article/K75432956
https://support.f5.com/csp/article/K82038789
https://support.f5.com/csp/article/K12403422
https://support.f5.com/csp/article/K05112543
https://support.f5.com/csp/article/K45325728

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

Identifikátor

Apache Tomcat WebSocket Client Hostname Verification Bypass Vulnerability

Popis

Spoločnosť Apache vydala bezpečnostné aktualizácie, ktoré opravujú viacero zraniteľností v produkte Apache Tomcat.
Prvá zraniteľnosť spočíva v chýbajúcom overovaní *hostname* parametrov v implementácii WebSocket klienta pre TLS (Transport Layer Security) spojenia a vzdialený neautentifikovaný útočník by ju prostredníctvom MITM (Man-In-The-Middle) útoku mohol zneužiť na obídenie bezpečnostných mechanizmov a vykonanie neoprávnených zmien v systéme.
Druhá zraniteľnosť spočíva v implementačnej chybe v NIO (Non-blocking I/O) a NIO2 konektoroch a vzdialený neautentifikovaný útočník by ju mohol zneužiť na neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

22.07.2018 (posledná aktualizácia 26.07.2018)

CVE

CVE-2018-8034, CVE-2018-8037

Zasiahnuté systémy

Tomcat 7.0.x verzie staršie ako 7.0.90
Tomcat 8.0.x verzie staršie ako 8.0.53
Tomcat 8.5.x verzie staršie ako 8.5.32
Tomcat 9.0.x verzie staršie ako 9.0.10

Následky

Neoprávnená zmena v systéme, Neopravený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

http://tomcat.apache.org/security-7.html
http://tomcat.apache.org/security-8.html
http://tomcat.apache.org/security-9.html
https://tools.cisco.com/security/center/viewAlert.x?alertId=58470
https://www.securitytracker.com/id/1041374

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre: 6.3**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Dell EMC NetWorker Clear-Text Authentication Over Network Vulnerability

Popis

Spoločnosť Dell vydala bezpečnostné aktualizácie, ktoré opravujú bezpečnostnú zraniteľnosť v produkte Dell EMC NetWorker.
Zraniteľnosť v komponente Rabbit MQ Advanced Message Queuing Protocol spočíva v chýbajúcom kryptografickom zabezpečení autentifikačných údajov v zasiahnutom systéme a umožňuje vzdialenému útočníkovi nachádzajúcemu sa v rovnakom sieťovom segmente získať prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

25.07.2018

CVE

CVE-2018-11050

Zasiahnuté systémy

Dell EMC NetWorker verzie staršie ako 9.1.1.9
Dell EMC NetWorker verzie staršie ako 9.2.1.4
Dell EMC NetWorker verzie staršie ako 18.1.0.2

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

http://seclists.org/fulldisclosure/2018/Jul/92

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre: 5.5**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

VMware Horizon View Agent, ESXi, Workstation and Fusion Multiple Vulnerabilities

Popis

Spoločnosť VMware vydala bezpečnostné aktualizácie, ktoré opravujú viacero bezpečnostných zraniteľností v produktoch Horizon View Agent, vSphere Hypervisor, Workstation a Fusion.
Zraniteľnosť v produktoch VMware vSphere Hypervisor, Workstation a Fusion spočíva v implementačnej chybe v komponente RPC Handler a lokálny autentifikovaný útočník by ju mohol zneužiť na vyvolanie pádu VM (Virtual Machine) a zneprístupnenie služieb.
Zraniteľnosť v produkte VMware Horizon View Agent spočíva v nedostatočnej implementácii bezpečnostných mechanizmov počas inštalácie aplikácie a lokálny autentifikovaný útočník by ju mohol zneužiť na získanie prístupu k prihlasovacím údajom špecifikovaným počas inštalácie.

Dátum prvého zverejnenia varovania

19.07.2018

CVE

CVE-2018-6971, CVE-2018-6972

Zasiahnuté systémy

VMware Horizon View Agent verzie staršie ako 7.5.1 (platforma Windows)
VMware vSphere Hypervisor verzie 5.5, 6.0, 6.5, 6.7 (všetky platformy)
VMware Workstation Pro / Player verzie staršie ako 14.1.2 (všetky platformy)
VMware Fusion Pro, Fusion verzie staršie ako 10.1.2 (platforma OSX)

Následky

Zneprístupnenie služby, Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.vmware.com/security/advisories/VMSA-2018-0018.html
https://securitytracker.com/id/1041356
https://securitytracker.com/id/1041357
https://securitytracker.com/id/1041358

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:
02049/2018/TS/OKB-102