# BEZPEČNOSTNÝ BULLETIN

Týždeň 03. 10. 2018 - 09. 10. 2018

## OBSAH BEZPEČNOSTNÉHO BULLETINU

| Č. | Identifikátor | Dôležitosť | CVSS Skóre |
|---|---|---|---|
| **01.** | Multiple Vulnerabilities in MikroTik routers | Vysoká | **8.8** |
| **02.** | Privilege Escalation in ROX II | Vysoká | **8.8** |
| **03.** | Cockpit CMS Multiple Vulnerabilities | Vysoká | **8.8** |
| **04.** | IBM Spectrum LSF and IBM Spectrum Symphony Multiple Vulnerabilities | Vysoká | **8.4** |
| **05.** | Teltonika RUT9XX Multiple Vulnerabilities | Vysoká | **8.2** |
| **06.** | WebKitGTK+ Multiple Vulnerabilities | Vysoká | **8.1** |
| **07.** | Multiple Vulnerabilities in liblouis Library for UBUNTU | Vysoká | **8.1** |
| **08.** | Microsoft Exchange Server Multiple Vulnerabilities | Vysoká | **8.0** |
| **09.** | Foxit Reader and Foxit PhantomPDF Multiple Vulnerabilities | Vysoká | **7.8** |
| **10.** | Intel QuickAssist Technology for Linux Remote code execution | Vysoká | **7.8** |
| **11.** | The Whale Browser Multiple Vulnerabilities | Vysoká | **7.8** |
| **12.** | WhatsApp Heap Corruption Vulnerability in RTP Packet Processing | Vysoká | **7.5** |
| **13.** | Insufficient Input Validation in BIOS Update Utility in Intel NUC FW Kits | Vysoká | **7.5** |
| **14.** | IBM Security Key Lifecycle Manager Multiple Vulnerabilities | Vysoká | **7.5** |
| **15.** | Ektron CMS Information Disclosure Vulnerability | Vysoká | **7.5** |
| **16.** | Microsoft Internet Explorer Remote Code Execution Vulnerabilities | Vysoká | **7.5** |
| **17.** | Intel Server Boards Firmware Advisory | Vysoká | **7.1** |
| **18.** | Microsoft Filter Manager Elevation Of Privilege Vulnerability | Vysoká | **7.0** |
| **19.** | Delta Industrial Automation TPEditor Multiple Vulnerabilities | Stredná | **6.6** |
| **20.** | Wireshark Multiple Denial of Service Vulnerabilities | Stredná | **6.5** |
| **21.** | MediaWiki Multiple Vulnerabilities | Stredná | **6.5** |
| **22.** | Dell Encryption and Dell Endpoint Security Suite Enterprise Security Policy Overwrite Vulnerability | Stredná | **6.4** |
| **23.** | Delta IElectronics ISPSoft Remote Code Execution Vulnerability | Stredná | **6.3** |
| **24.** | OPC Foundation UA Client Vulnerability | Stredná | **5.3** |
| **25.** | Intel NVMe and Intel RSTe Vulnerability | Stredná | **5.0** |
| **26.** | Windows Server DNS Global Blocklist Vulnerability | Stredná | **4.3** |

**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-152

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

## Identifikátor

Multiple Vulnerabilities in MikroTik routers

## Popis

Bezpečnostní výskumníci z Tenable Research zverejnili Proof-of-Concept kód pre nový útočný vektor zneužívajúci zraniteľnosť CVE-2018-14847 nachádzajúci sa v komponente Winbox na routeroch MikroTik. Vzdialený útočník by ju mohol zneužiť na vykonanie škodlivého kódu a získanie úplnej kontroly nad zasiahnutými zariadeniami.
Ostatné zraniteľnosti by vzdialený autentifikovaný útočník mohol zneužiť na vykonanie škodlivého kódu alebo zneprístupnenie služby.

## Dátum prvého zverejnenia varovania

07.10.2018

## CVE

CVE-2018-1156, CVE-2018-1157, CVE-2018-1158, CVE-2018-1159, CVE-2018-14847

## Zasiahnuté systémy

Mikrotik RouterOS firmvér verzie staršie ako 6.42.7 a 6.40.9

## 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://blog.mikrotik.com/security/new-exploit-for-mikrotik-router-winbox-vulnerability.html
https://blog.mikrotik.com/security/security-issues-discovered-by-tenable.html
https://github.com/tenable/routeros/tree/master/poc/bytheway
https://www.tenable.com/blog/tenable-research-advisory-multiple-vulnerabilities-discovered-in-mikrotiks-routeros

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

## Identifikátor

Privilege Escalation in ROX II

## Popis

Spoločnosť Siemens vydala bezpečnostnú aktualizáciu, ktorá opravuje dve zraniteľnosti v produkte ROX II.
Prvú zraniteľnosť by vzdialený autentifikovaný útočník s používateľským účtom s nízkymi oprávneniami mohol zneužiť na eskaláciu privilégií a získanie úplnej kontroly nad zasiahnutým systémom.
Druhú zraniteľnosť by vzdialený autentifikovaný útočník s SSH prístupom ku systému mohol zneužiť na vykonanie škodlivého kódu.

## Dátum prvého zverejnenia varovania

09.10.2018

## CVE

CVE-2018-13801, CVE-2018-13802

## Zasiahnuté systémy

SSA ROX II verzie staršie ako 2.12.1

## Následky

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

## Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

## Zdroje

https://support.industry.siemens.com/cs/us/en/view/109760683
https://cert-portal.siemens.com/productcert/pdf/ssa-493830.pdf

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

## Identifikátor

Cockpit CMS Multiple Vulnerabilities

## Popis

Vývojári systému pre správu obsahu Cockpit CMS vydali bezpečnostnú aktualizáciu, ktorá opravuje viacero bezpečnostných zraniteľností.
Prvá zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a vzdialený neautentifikovaný útočník by ju prostredníctvom podvrhnutia požiadaviek obsahujúcich /../ sekvenciu na /cockpit/media/api mohol zneužiť na získanie neoprávneného prístupu k citlivým údajom.
Ostatné zraniteľnosti by vzdialený neautentifikovaný útočník mohol zneužiť na vykonanie CSRF (Cross-Site Request Forgery) a XSS (Cross-Site Scripting) útokov a následné vykonanie škodlivého kódu.

## Dátum prvého zverejnenia varovania

10.10.2018

## CVE

CVE-2018-15538, CVE-2018-15539, CVE-2018-15540

## Zasiahnuté systémy

Cockpit CMS verzie staršie ako 0.6.2

## Následky

Vykonanie škodlivého kódu, Neoprávnený prístup k citlivým údajom

## Odporúčania

Odporúčame uistiť sa, či vaše webové stránky nie sú založené na systéme pre správu obsahu Cockpit v zraniteľnej verzii. V prípade, že áno, odporúčame vykonať aktualizáciu redakčného systému na najnovšiu verziu.

## Zdroje

https://seclists.org/fulldisclosure/2018/Oct/30

| | | | | | |
|---|---|---|---|---|---|
| **Dôležitosť** | ☐ **Nízka** | ☐ **Stredná** | ☒ **Vysoká** | ☐ **Kritická** | **CVSS skóre: 8.4** |
| **Klasifikácia** | ☒ **Neutajované / TLP(WHITE)** | | ☐ **Vyhradené** | ☐ **Dôverné** | ☐ **Tajné** |
| **Kód sektora (dopad)** | | | | | |

## Identifikátor

IBM Spectrum LSF and IBM Spectrum Symphony Multiple Vulnerabilities

## Popis

Spoločnosť IBM vydala bezpečnostné aktualizácie na svoje produkty, ktoré opravujú viacero bezpečnostných zraniteľností.
Zraniteľnosť v produkte IBM Spectrum LSF spočíva v nesprávnej konfigurácii oprávnení na prístup k súborom obsahujúcim citlivé údaje a lokálny neautentifikovaný útočník by ju mohol zneužiť na eskaláciu privilégií a získanie úplnej kontroly nad zasiahnutým systémom.
Zraniteľnosti v produkte IBM Spectrum Symphony sa nachádzajú v komponente WebGui a vzdialený autentifikovaný útočník by ich mohol zneužiť na realizáciu XSS (Cross-Site Scripting) útokov, vykonanie škodlivého kódu a neoprávnený prístup k údajom uloženým v cookies, vrátane autentifikačných údajov.

## Dátum prvého zverejnenia varovania

11.10.2018

## CVE

CVE-2018-1706, CVE-2018-1708, CVE-2018-1724

## Zasiahnuté systémy

IBM Spectrum LSF verzie 9.1.1 9.1.2, 9.1.3 a 10.1
IBM Spectrum Symphony verzie 7.1.2 a 7.2.0.2

## Následky

Vykonanie škodlivého kódu, Eskalácia privilégií, Neoprávnený prístup k citlivým údajom

## Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

## Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/147439
https://exchange.xforce.ibmcloud.com/vulnerabilities/146343
https://exchange.xforce.ibmcloud.com/vulnerabilities/146341

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

## Identifikátor

Teltonika RUT9XX Multiple Vulnerabilities

## Popis

Spoločnosť Teltonika vydala bezpečnostné aktualizácie firmwaru routrov Teltonika RUT9XX, ktoré opravujú viacero zraniteľností.
Prvá zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov v hotspotlogin.cgi a vzdialený neautentifikovaný útočník by ju mohol zneužiť na realizáciu XSS (Cross-Site Scripting) útoku, vykonanie škodlivého kódu a získanie prístupu k údajom uloženým v cookies, vrátane autentifikačných údajov.
Druhá zraniteľnosť spočíva v chýbajúcom zabezpečení sériového rozhrania a neautentifikovaný útočník s fyzickým prístupom by ju mohol zneužiť na získanie administrátorského prístupu k zariadeniu.
Na uvedené zraniteľnosti je dostupný Proof-of-Concept kód.

## Dátum prvého zverejnenia varovania

11.10.2018

## CVE

CVE-2018-17533, CVE-2018-17534

## Zasiahnuté systémy

RUT9XX routre verzie staršie ako 00.05.01.1
RUT9XX routre verzie staršie ako 00.04.233

## Následky

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

## Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

## Zdroje

https://seclists.org/fulldisclosure/2018/Oct/28
https://seclists.org/fulldisclosure/2018/Oct/29

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

## Identifikátor

WebKitGTK+ Multiple Vulnerabilities

## Popis

Vývojári webových a JavaScriptových enginov WebKitGTK+ pre operačné systémy Ubuntu 18.04 LTS vydali bezpečnostné aktualizácie, ktoré opravujú viacero chýb a viacero bezpečnostných zraniteľností. Uvedené zraniteľnosti by vzdialený neautentifikovaný útočník prostredníctvom podvrhnutia škodlivého webového obsahu mohol zneužiť na realizáciu XSS (Cross-Site Scripting) útokov, vykonanie škodlivého kódu alebo zneprístupnenie služby.

## Dátum prvého zverejnenia varovania

03.10.2018

## CVE

CVE-2018-4191, CVE-2018-4197, CVE-2018-4207, CVE-2018-4208, CVE-2018-4209, CVE-2018-4210, CVE-2018-4212, CVE-2018-4213, CVE-2018-4299, CVE-2018-4306, CVE-2018-4309, CVE-2018-4311, CVE-2018-4312, CVE-2018-4314, CVE-2018-4315, CVE-2018-4316, CVE-2018-4317, CVE-2018-4318, CVE-2018-4319, CVE-2018-4323, CVE-2018-4328, CVE-2018-4358, CVE-2018-4359, CVE-2018-4361

## Zasiahnuté systémy

libjavascriptcoregtk verzie staršie ako 4.0-18 pre OS Ubuntu 18.04 LTS
libwebkit2gtk verzie staršie ako 4.0-37 pre OS Ubuntu 18.04 LTS

## Následky

Vykonanie škodlivého kódu, Zneprístupnenie služby

## Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

## Zdroje

https://usn.ubuntu.com/3781-1/

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

## Identifikátor

Multiple Vulnerabilities in liblouis Library for UBUNTU

## Popis

Vývojári knižnice liblouis slúžiacej pre spracovanie Braillovho písma vydali bezpečnostné aktualizácie, ktoré opravujú viacero bezpečnostných zraniteľností.
Bližšie nešpecifikované zraniteľnosti by vzdialený útočník prostredníctvom podvrhnutia špeciálne vytvorených súborov mohol zneužiť na vykonanie škodlivého kódu alebo zneprístupnenie služby.

## Dátum prvého zverejnenia varovania

03.10.2018

## CVE

CVE-2018-12085, CVE-2018-17294

## Zasiahnuté systémy

liblouis-bin, liblouis14 pre OS Ubuntu 18.04 LTS
liblouis-bin, liblouis9 pre OS Ubuntu 16.04 LTS
liblouis-bin, liblouis2 pre OS Ubuntu 14.04 LTS

## Následky

Vykonanie škodlivého kódu, Zneprístupnenie služby

## Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

## Zdroje

https://usn.ubuntu.com/usn/usn-3782-1
http://www.linuxsecurity.com/content/view/214273?rdf

| | | | | | |
|---|---|---|---|---|---|
| **Dôležitosť** | ☐ **Nízka** | ☐ **Stredná** | ☒ **Vysoká** | ☐ **Kritická** | **CVSS skóre: 8.0** |
| **Klasifikácia** | ☒ **Neutajované / TLP(WHITE)** | | ☐ **Vyhradené** | ☐ **Dôverné** | ☐ **Tajné** |
| **Kód sektora (dopad)** | | | | | |

## Identifikátor

Microsoft Exchange Server Multiple Vulnerabilities

## Popis

Spoločnosť Microsoft vydala aktualizáciu svojho produktu Microsoft Exchange Server, ktorá opravuje viacero bezpečnostných zraniteľností.
Prvá zraniteľnosť spočíva v implementačnej chybe parsera e-mailových správ a vzdialený neautentifikovaný útočník by ju prostredníctvom podvrhnutia špeciálne vytvorených e-mailov mohol zneužiť na vykonanie škodlivého kódu.
Druhá zraniteľnosť sa nachádza v Microsoft Exchange Outlook Web Access (OWA) a vzdialený neautentifikovaný útočník by ju prostredníctvom podvrhnutia škodlivého obsahu mohol zneužiť na získanie prístupu k citlivým údajom.

## Dátum prvého zverejnenia varovania

09.10.2018

## CVE

CVE-2018-8265, CVE-2018-8448

## Zasiahnuté systémy

Microsoft Exchange Server 2013 Cumulative Update 21
Microsoft Exchange Server 2016 Cumulative Update 10

## Následky

Vykonanie škodlivého kódu, Neoprávnený prístup k citlivým údajom

## Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

## Zdroje

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8265
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8448
https://securitytracker.com/id/1041836

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

## Identifikátor

Foxit Reader and Foxit PhantomPDF Multiple Vulnerabilities

## Popis

Spoločnost Foxit vydala bezpečnostné aktualizácie, ktoré opravujú viacero bezpečnostných zraniteľností v produktoch Foxit Reader a Foxit PhantomPDF.
Prvá zraniteľnosť spočíva v nedostatočnom overovaní existencie objektu pred vykonaním operácií v metóde XFA setInterval. Druhá zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov pri konverzii HTML súborov do PDF. Uvedené zraniteľnosti by vzdialený neautentifikovaný útočník mohol zneužiť na vykonanie škodlivého kódu v kontexte aktuálne bežiaceho procesu.
Zneužitie týchto zraniteľností vyžaduje interakciu používateľa v tom, že cieľ musí navštíviť škodlivú stránku alebo otvoriť škodlivý súbor.

## Dátum prvého zverejnenia varovania

11.10.2018

## CVE

CVE-2018-17628, CVE-2018-17693

## Zasiahnuté systémy

Foxit Reader pred V 9.3 a Foxit PhantomPDF pred V 9.3

## 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.

## Zdroje

https://www.zerodayinitiative.com/advisories/ZDI-18-1230/
https://www.zerodayinitiative.com/advisories/ZDI-18-1182/

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

## Identifikátor

Intel QuickAssist Technology for Linux Remote code execution

## Popis

Spoločnosť Intel vydala aktualizáciu, ktorá opravuje bezpečnostnú zraniteľnosť v produkte Intel QuickAssist Technology for Linux.
Zraniteľnosť spočíva v nedostatočnej implementácii mechanizmov riadenia prístupu a lokálny autentifikovaný útočník by ju mohol zneužiť na získanie neoprávneného prístupu k citlivým údajom.

## Dátum prvého zverejnenia varovania

09.10.2018

## CVE

CVE-2018-12193

## Zasiahnuté systémy

Intel QuickAssist Technology for Linux verzie staršie ako 4.2

## Následky

Neoprávnený prístup k citlivým údajom

## Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých systémov.

## Zdroje

https://01.org/security/advisories/intel-oss-10005
https://nvd.nist.gov/vuln/detail/CVE-2018-12193

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

## Identifikátor

The Whale Browser Multiple Vulnerabilities

## Popis

Spoločnosť NAVER informuje o bezpečnostných zraniteľnostiach vo webovom prehliadači Whale.
Prvá zraniteľnosť CVE-2018-12449 spočíva v nesprávnej implementácii nahrávania dynamických knižníc DLL inštalátorom a lokálny neautentifikovaný útočník by ju prostredníctvom podvrhnutia špeciálne vytvorených DLL súborov mohol zneužiť na vykonanie škodlivého kódu.
Druhá zraniteľnosť spočíva v nesprávnom zobrazovaní informácií pri navštívení non-http stránok, pre ktoré prehliadač v lište nezobrazuje informácie o URL, ale len názov webovej stránky. Uvedenú zraniteľnosť by útočník mohol zneužiť na podvrhnutie škodlivého webového obsahu.

## Dátum prvého zverejnenia varovania

11.10.2018

## CVE

CVE-2018-12448, CVE-2018-12449

## Zasiahnuté systémy

Whale Browser inštalátor verzie 0.4.3.0 a staršie (CVE-2018-12449)
Whale Browser verzie 1.3.48.4 a staršie

## Následky

Vykonanie škodlivého kódu

## Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov. Tiež odporúčame poučiť používateľov, aby neotvárali odkazy a prílohy z nedôveryhodných zdrojov.

## Zdroje

https://cve.naver.com/detail/cve-2018-12449
https://cve.naver.com/detail/cve-2018-12448
https://nvd.nist.gov/vuln/detail/CVE-2018-12449
https://nvd.nist.gov/vuln/detail/CVE-2018-12448

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

## Identifikátor

WhatsApp Heap Corruption Vulnerability in RTP Packet Processing

## Popis

Spoločnosť WhatsApp Inc. vydala bezpečnostnú aktualizáciu, ktorá opravuje bezpečnostnú zraniteľnosť v produkte WhatsApp.
Bližšie nešpecifikovanú implementačnú chybu by vzdialený neautentifikovaný útočník prostredníctvom podvrhnutia špeciálne vytvorených RTP paketov mohol vyvolať pád aplikácie a spôsobiť tak zneprístupnenie služby.
Na uvedenú zraniteľnosť je v súčasnosti dostupný Proof-of-Concept kód.

## Dátum prvého zverejnenia varovania

10.10.2018

## CVE

-

## Zasiahnuté systémy

WhatsApp pre platformu Android a iPhone

## Následky

Zneprístupnenie služby

## Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

## Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/151079

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

## Identifikátor

Insufficient Input Validation in BIOS Update Utility in Intel NUC FW Kits

## Popis

Spoločnosť Intel vydala bezpečnostné aktualizácie na svoje produkty, ktoré opravujú bezpečnostnú zraniteľnosť v Intel® NUC Firmware Kits.
Zraniteľnosť spočíva v nedostatočnom overovaní vstupov v nástroji na aktualizáciu systému BIOS a lokálny autentifikovaný útočník by ju mohol zneužiť na zneprístupnenie služby alebo neoprávnený prístup k citlivým údajom.

## Dátum prvého zverejnenia varovania

09.10.2018

## CVE

CVE-2018-12158

## Zasiahnuté systémy

Intel® NUC Firmware Kits vydané pred 24.05.2018.

## Následky

Zneprístupnenie služby, Neoprávnený prístup k citlivým údajom

## Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

## Zdroje

https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00168.html
https://nvd.nist.gov/vuln/detail/CVE-2018-12158

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

## Identifikátor

IBM Security Key Lifecycle Manager Multiple Vulnerabilities

## Popis

Spoločnosť IBM vydala bezpečnostnú aktualizáciu, ktorý obsahuje viacero zraniteľností v produkte IBM Security Key Lifecycle Manager.
Prvú zraniteľnosť by vzdialený autentifikovaný útočník mohol zneužiť na získanie prístupu k citlivým údajom alebo narušenie integrity systému.
Druhú zraniteľnosť by vzdialený neautentifikovaný útočník mohol zneužiť na reštartovanie SKLM servera.
Zraniteľnosti spočívajú v nedostatočnej implementácii mechanizmov autentifikácie.

## Dátum prvého zverejnenia varovania

11.10.2018

## CVE

CVE-2018-1738, CVE-2018-1745

## Zasiahnuté systémy

IBM Security Key Lifecycle Manager verzie 2.6 - 2.6.0.4 (len CVE-2018-1738)
IBM Security Key Lifecycle Manager verzie 2.7 až 2.7.0.3
IBM Security Key Lifecycle Manager verzie 3.0 až 3.0.0.1

## Následky

Zneprístupnenie služby, Neoprávnený prístup k citlivým údajom, Neoprávnená zmena v systéme

## Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

## Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/148424
https://exchange.xforce.ibmcloud.com/vulnerabilities/147907
https://www-01.ibm.com/support/docview.wss?uid=ibm10733355
https://www-01.ibm.com/support/docview.wss?uid=ibm10733309

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

## Identifikátor

Ektron CMS Information Disclosure Vulnerability

## Popis

Spoločnosť Episerver Inc. vydala bezpečnostnú aktualizáciu, ktorá opravuje bezpečnostnú zraniteľnosť v systéme na správu obsahu Ektron CMS.
Zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov v activateuser.aspx a vzdialený neautentifikovaný útočník by ju mohol zneužiť na aktiváciu používateľov a získanie neoprávneného prístupu do systému.

## Dátum prvého zverejnenia varovania

09.10.2018

## CVE

CVE-2018–12596

## Zasiahnuté systémy

Ektron Content Management System (CMS) 9.20 SP2

## Následky

Neoprávnený prístup do systému

## Odporúčania

Odporúčame uistiť sa, či vaše webové stránky nie sú založené na systéme pre správu obsahu Ektron v zraniteľnej verzii. V prípade, že áno, odporúčame vykonať aktualizáciu redakčného systému na najnovšiu verziu.

## Zdroje

https://github.com/alt3kx/CVE-2018-12596
https://www.exploit-db.com/exploits/45577/
https://seclists.org/fulldisclosure/2018/Oct/15

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

## Identifikátor

Microsoft Internet Explorer Remote Code Execution Vulnerabilities

## Popis

Spoločnosť Microsoft vydala bezpečnostné aktualizácie, ktoré opravujú viacero bezpečnostných zraniteľností v internetovom prehliadači Internet Explorer 11.
Zraniteľnosti sú spôsobená implementačnou chybou, ktorá spočíva v nesprávnom pristupovaní k objektom v pamäti. Vzdialený neautentifikovaný útočník by ich prostredníctvom podvrhnutia škodlivého webového obsahu mohol zneužiť na vykonanie škodlivého kódu v kontexte prihláseného používateľa.

## Dátum prvého zverejnenia varovania

10.10.2018

## CVE

CVE-2018-8460, CVE-2018-8491

## Zasiahnuté systémy

Internet Explorer 11

## Následky

Vzdialené vykonanie kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému

## Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov. Tiež odporúčame poučiť používateľov, aby neotvárali odkazy a prílohy z nedôveryhodných zdrojov.

## Zdroje

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8460
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8491

| | | | | | |
|---|---|---|---|---|---|
| **Dôležitosť** | ☐ **Nízka** | ☐ **Stredná** | ☒ **Vysoká** | ☐ **Kritická** | **CVSS skóre: 7.1** |
| **Klasifikácia** | ☒ **Neutajované / TLP(WHITE)** | | ☐ **Vyhradené** | ☐ **Dôverné** | ☐ **Tajné** |
| **Kód sektora (dopad)** | | | | | |

## Identifikátor

Intel Server Boards Firmware Advisory

## Popis

Spoločnosť Intel vydala bezpečnostné aktualizácie na svoje produkty, ktoré opravujú bezpečnostnú zraniteľnosť vo firméri zariadení Intel Server Board, Intel Server System a Intel Compute Module. Bližšie nešpecifikovanú zraniteľnosť by neautentifikovaný útočník s fyzickým prístupom z zariadeniam mohol zneužiť na vykonanie škodlivého kódu. Vykonaním škodlivého kódu by útočník mohol získať neoprávnený prístup k citlivým údajom, eskalovať svoje privilégiá alebo spôsobiť zneprístupnenie služby.

## Dátum prvého zverejnenia varovania

09.10.2018

## CVE

CVE-2018-12173

## Zasiahnuté systémy

Zasiahnuté sú nasledujúce zariadenia s firmwarom verzie staršej ako 00.01.0014:
Intel Server Board S2600BP Family
Intel Compute Module HNS2600BP Family
Intel Server System H2000G Family
Intel Server Board S2600WF Family
Intel Server System R2000WF Family
Intel Server System R1000WF Family
Intel Server Board S2600ST Family
Intel Server Board S2600BPR Family
Intel Compute Module HNS2600BPR Family
Intel Server System H2000GR Family
Intel Server Board S2600WFR Family
Intel Server System R2000WFR Family
Intel Server System R1000WFR Family
Intel Server Board S2600STR Family

## Následky

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

## Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

## Zdroje

https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00179.html
https://nvd.nist.gov/vuln/detail/CVE-2018-12173

| | | | | | |
|---|---|---|---|---|---|
| **Dôležitosť** | ☐ **Nízka** | ☐ **Stredná** | ☒ **Vysoká** | ☐ **Kritická** | **CVSS skóre: 7.0** |
| **Klasifikácia** | ☒ **Neutajované / TLP(WHITE)** | | ☐ **Vyhradené** | ☐ **Dôverné** | ☐ **Tajné** |
| **Kód sektora (dopad)** | | | | | |

## Identifikátor

Microsoft Filter Manager Elevation Of Privilege Vulnerability

## Popis

Spoločnosť Microsoft vydala bezpečnostné aktualizácie, ktoré opravujú bezpečnostnú zraniteľnosť v produktoch Microsoft Windows.
Zraniteľnosť sa nachádza v komponente Microsoft Filter Manager a spočíva v nesprávnej implementácii prístupu k objektom v pamäti. Lokálny autentifikovaný útočník by ju mohol zneužiť na vykonanie škodlivého kódu, eskaláciu privilégií a získanie kontroly nad zasiahnutým systémom.

## Dátum prvého zverejnenia varovania

10.10.2018

## CVE

CVE-2018-8333

## Zasiahnuté systémy

Microsoft Windows 10
Microsoft Windows 8.1
Microsoft Windows 7
Microsoft Windows Server 2008
Microsoft Windows Server 2012
Microsoft Windows Server 2016
Microsoft Windows Server 2019

## Následky

Vykonanie škodlivého kódu, Eskalácia privilégií

## Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

## Zdroje

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8333
https://www.zerodayinitiative.com/advisories/ZDI-18-1135/

| | | | | | |
|---|---|---|---|---|---|
| **Dôležitosť** | ☐ **Nízka** | ☒ **Stredná** | ☐ **Vysoká** | ☐ **Kritická** | **CVSS skóre:** 6.6 |
| **Klasifikácia** | ☒ **Neutajované / TLP(WHITE)** | | ☐ **Vyhradené** | ☐ **Dôverné** | ☐ **Tajné** |
| **Kód sektora (dopad)** | | | | | |

## Identifikátor

Delta Industrial Automation TPEditor Multiple Vulnerabilities

## Popis

Spoločnosť Delta Electronics vydala bezpečnostné aktualizácie, ktoré opravujú viacero zraniteľností v produkte Delta Industrial Automation TPEditor.
Zraniteľnosti spočívajú v nedostatočnom overovaní používateľských vstupov a lokálny neautentifikovaný útočník by ju prostredníctvom podvrhnutia špeciálne vytvorených súborov mohol zneužiť na vyvolenie pretečenia pamäte, zneprístupnenie služby a potenciálne vykonanie škodlivého kódu.

## Dátum prvého zverejnenia varovania

11.10.2018

## CVE

CVE-2018-17927, CVE-2018-17929

## Zasiahnuté systémy

TPEditor verzie 1.90 a staršie

## Následky

Vykonanie škodlivého kódu, Zneprístupnenie služby

## Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov. Tiež odporúčame poučiť používateľov, aby neotvárali súbory z nedôveryhodných zdrojov. Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od Internetu.

## Zdroje

https://ics-cert.us-cert.gov/advisories/ICSA-18-284-03

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

## Identifikátor

Wireshark Multiple Denial of Service Vulnerabilities

## Popis

Vývojári analytického nástroja Wireshark vydali aktualizáciu svojho produktu, ktorá opravuje viacero bezpečnostných zraniteľností.
Uvedené zraniteľnosti by vzdialený neautentifikovaný útočník prostredníctvom podvrhnutia špeciálne vytvorených súborov alebo sieťovej prevádzky mohol zneužiť na zneprístupnenie služieb na zasiahnutom systéme.
Zraniteľnosti sa nachádzajú v komponentoch:
- CoAP dissector (epan/dissectors/packet-coap.c)
- OpcUa dissector
- MS-WSP dissector
- Steam IHS Discovery dissector

## Dátum prvého zverejnenia varovania

10.10.2018

## CVE

CVE-2018-12086, CVE-2018-18225, CVE-2018-18226, CVE-2018-18227

## Zasiahnuté systémy

Wireshark verzie 2.6.0 až 2.6.3
Wireshark verzie 2.4.0 až 2.4.9

## Následky

Zneprístupnenie služby

## Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

## Zdroje

https://www.wireshark.org/security/wnpa-sec-2018-50.html
https://www.wireshark.org/security/wnpa-sec-2018-49.html
https://www.wireshark.org/security/wnpa-sec-2018-48.html
https://www.wireshark.org/security/wnpa-sec-2018-47.html

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

## Identifikátor

MediaWiki Multiple Vulnerabilities

## Popis

Vývojári wiki softwaru WikiMedia vydali bezpečnostné aktualizácie na svoj produkt, ktoré opravujú 4 bezpečnostné zraniteľnosti nachádzajúce sa v jadre systému.
Uvedené zraniteľnosti by vzdialený autentifikovaný útočník mohol zneužiť na získanie neoprávneného prístupu k citlivým údajom.

## Dátum prvého zverejnenia varovania

21.09.2018

## CVE

CVE-2018-0503, CVE-2018-0504, CVE-2018-0505, CVE-2018-13258

## Zasiahnuté systémy

MediaWiki verzie staršie ako 1.31.1, 1.30.1, 1.29.3 a 1.27.5

## Následky

Neoprávnený prístup k citlivým údajom

## Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

## Zdroje

https://lists.wikimedia.org/pipermail/mediawiki-announce/2018-September/000223.html
https://www.securitytracker.com/id/1041695

| | | | | | |
|---|---|---|---|---|---|
| **Dôležitosť** | ☐ **Nízka** | ☒ **Stredná** | ☐ **Vysoká** | ☐ **Kritická** | **CVSS skóre:** 6.4 |
| **Klasifikácia** | ☒ **Neutajované / TLP(WHITE)** | | ☐ **Vyhradené** | ☐ **Dôverné** | ☐ **Tajné** |
| **Kód sektora (dopad)** | | | | | |

## Identifikátor

Dell Encryption and Dell Endpoint Security Suite Enterprise Security Policy Overwrite Vulnerability

## Popis

Spoločnosť Dell vydala bezpečnostné aktualizácie, ktoré opravujú viacero bezpečnostných zraniteľností v produktoch Dell Encryption a Dell Endpoint Security Suite Enterprise.
Pri inštalácii komponentu Encryption Management Agent alebo aplikácie EMAgent dochádza k nastaveniu objektu "Minimum Password Length" na hodnotu 1. Objekt špecifikuje minimálnu dĺžku používateľských hesiel. Lokálny autentifikovaný útočník by uvedenú zraniteľnosť mohol zneužiť na obídenie pravidiel bezpečnostnej politiky organizácie a potenciálne získanie neoprávneného prístupu do systému.

## Dátum prvého zverejnenia varovania

11.10.2018

## CVE

CVE-2018-15766

## Zasiahnuté systémy

Dell Endpoint Security Suite Enterprise verzie staršie ako 2.0.1
Dell Encryption verzie staršie ako 10.0.1

## Následky

Neoprávnený prístup do systému

## Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

## Zdroje

https://www.dell.com/support/article/us/en/04/sln313561/dell-encryption-and-dell-endpoint-security-suite-enterprise-security-policy-overwrite-vulnerability
https://nvd.nist.gov/vuln/detail/CVE-2018-15766

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

## Identifikátor

Delta IElectronics ISPSoft Remote Code Execution Vulnerability

## Popis

Spoločnosť Delta Electronics vydala bezpečnostnú aktualizáciu, ktorá opravuje bezpečnostnú zraniteľnosť v produkte Industrial Automation slúžiacom na programovanie PLC zariadení.
Zraniteľnosť spočíva v nesprávnej implementácii parsera DVP súborov a vzdialený neautentifikovaný útočník by ju prostredníctvom podvrhnutia špeciálne vytvorených DVP súborov mohol zneužiť na vykonanie škodlivého kódu v kontexte bežiaceho procesu.

## Dátum prvého zverejnenia varovania

10.10.2018

## CVE

CVE-2018-14800

## Zasiahnuté systémy

ISPSoft vezie 3.0.5 a staršie

## Následky

Vykonanie škodlivého kódu

## Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov. Tiež odporúčame poučiť používateľov, aby neotvárali odkazy a prílohy z nedôveryhodných zdrojov. Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od Internetu.

## Zdroje

https://ics-cert.us-cert.gov/advisories/ICSA-18-275-01
https://www.zerodayinitiative.com/advisories/ZDI-18-1139/

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

## Identifikátor

OPC Foundation UA Client Vulnerability

## Popis

Vývojári z OPC Foundation vydali bezpečnostnú aktualizáciu, ktorá opravuje zraniteľnosť v produkte OPC UA.
Zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov, ktorá umožňuje využitie nedôveryhodných certifikátov na šifrovanie komunikácie medzi klientom a serverom aplikácie OPC UA. Uvedenú zraniteľnosť by neautentifikovaný útočník s fyzickým prístupom k sieťovej infraštruktúre mohol zneužiť na dešifrovanie zabezpečenej komunikácie a získať neoprávnený prístup k citlivým údajom.
Uvedenú zraniteľnosť je možné zneužiť len na klientskych aplikáciách, ktoré počas budovania relácie s parametrom "SecurityMode None" využívajú šifrovanie UserIdentityToken.

## Dátum prvého zverejnenia varovania

03.10.2018

## CVE

CVE-2018-12087

## Zasiahnuté systémy

OPC UA Client verzie vydané pred 17.07.2018

## Následky

Neoprávnený prístup k citlivým údajom

## Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

## Zdroje

https://opcfoundation-onlineapplications.org/faq/SecurityBulletins/OPC_Foundation_Security_Bulletin_CVE-2018-12087.pdf
https://nvd.nist.gov/vuln/detail/CVE-2018-12087

| | | | | | |
|---|---|---|---|---|---|
| **Dôležitosť** | ☐ **Nízka** | ☒ **Stredná** | ☐ **Vysoká** | ☐ **Kritická** | **CVSS skóre:** 5.0 |
| **Klasifikácia** | ☒ **Neutajované / TLP(WHITE)** | | ☐ **Vyhradené** | ☐ **Dôverné** | ☐ **Tajné** |
| **Kód sektora (dopad)** | | | | | |

## Identifikátor

Intel NVMe and Intel RSTe Vulnerability

## Popis

Spoločnosť Intel vydala bezpečnostné aktualizácie, ktoré opravujú bezpečnostnú zraniteľnosť v produktoch Intel NVMe a Intel RSTe.
Bezpečnostná zraniteľnosť sa nachádza v inštalačných balíčkoch ovládačov a lokálny autentifikovaný útočník by ju mohol zneužiť na eskaláciu privilégií.

## Dátum prvého zverejnenia varovania

10.10.2018

## CVE

CVE-2018-12131

## Zasiahnuté systémy

Intel Client NVMe verzie 4.0.0.1006 a staršie
Datacenter NVMe verzie 4.0.0.1006 a staršie
Intel RSTe verzie 4.7.0.2082 a staršie

## Následky

Eskalácia privilégií

## Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých systémov.

## Zdroje

https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00154.html
https://nvd.nist.gov/vuln/detail/CVE-2018-12131

| | | | | | |
|---|---|---|---|---|---|
| **Dôležitosť** | ☐ **Nízka** | ☒ **Stredná** | ☐ **Vysoká** | ☐ **Kritická** | **CVSS skóre: 4.3** |
| **Klasifikácia** | ☒ **Neutajované / TLP(WHITE)** | | ☐ **Vyhradené** | ☐ **Dôverné** | ☐ **Tajné** |
| **Kód sektora (dopad)** | | | | | |

## Identifikátor

Windows Server DNS Global Blocklist Vulnerability

## Popis

Spoločnosť Microsoft vydala aktualizácie na svoje produkty Windows Server 2012 R2, Windows Server 2008, Windows Server 2012, Windows Server 2019, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Server, ktoré opravujú bezpečnostnú zraniteľnosť vo funkcii DNS Global Blocklist. Zraniteľnosť by vzdialený autentifikovaný útočník mohol zneužiť na obídenie bezpečnostných mechanizmov a presmerovanie sieťovej prevádzky prostredníctvom DNS.

## Dátum prvého zverejnenia varovania

09.10.2018

## CVE

CVE-2018-8320

## Zasiahnuté systémy

Windows Server 2012 R2, Windows Server 2008, Windows Server 2012, Windows Server 2019, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servery.

## Následky

Neoprávnená zmena v systéme

## Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov, aplikovať firewallové pravidlá a limitovať prístup k zasiahnutým zariadeniam a jeho funkciám zavedením zoznamu pre riadenie prístupov (ACL).

## Zdroje

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8320