BEZPEČNOSTNÝ BULLETIN

Týždeň 02. 10. 2019 - 08. 10. 2019

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	WhatsApp for Android zraniteľnosť	Vysoká	**8.8**
02.	Cisco produkty viacero zraniteľností	Vysoká	**8.8**
03.	Apple iCloud a macOS zraniteľnosti	Vysoká	**8.8**
04.	Zraniteľnosť produktov Yokogawa	Vysoká	**8.4**
05.	Android zero-day zraniteľnosť	Vysoká	**8.0**
06.	vBulletin zraniteľnosti	Vysoká	**7.9**
07.	Ruby zraniteľnosti	Vysoká	**7.8**
08.	PuTTY zraniteľnosti	Vysoká	**7.5**
09.	Signal for Android zraniteľnosť	Vysoká	**7.5**
10.	IBM Security Directory Server zraniteľnosti	Vysoká	**7.5**
11.	Moxa EDR 810 zraniteľnosti	Vysoká	**7.2**

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/SK-CERT-239

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

Identifikátor

WhatsApp for Android zraniteľnosť

Popis

Spoločnosť Facebook vydala bezpečnostnú aktualizáciu na svoj produkt WhatsApp for Android, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť v knižnici libpl_droidsonroids_gif.so je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených gif súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.
Proof-of-concept kód popisujúci danú zraniteľnosť je voľne dostupný.

Dátum prvého zverejnenia varovania

02.10.2019

CVE

CVE-2019-11932

Zasiahnuté systémy

android gif drawable verzie staršie ako 1.2.18
WhatsApp for Android verzie staršie ako 2.19.244

Následky

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

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://awakened1712.github.io/hacking/hacking-whatsapp-gif-rce/
https://thehackernews.com/2019/10/whatsapp-rce-vulnerability.html
https://www.facebook.com/security/advisories/cve-2019-11932

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

Identifikátor

Cisco produkty viacero zraniteľností

Popis

Spoločnosť Cisco vydala aktualizácie na väčšie množstvo svojich produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšie bezpečnostné zraniteľnosti v produkte Firepower sú spôsobené nedostatočným overovaním používateľských vstupov a umožňujú vzdialenému, autentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

02.10.2019

CVE

CVE-2019-12630, CVE-2019-12631, CVE-2019-12673, CVE-2019-12674, CVE-2019-12675, CVE-2019-12676, CVE-2019-12677, CVE-2019-12678, CVE-2019-12679, CVE-2019-12680, CVE-2019-12681, CVE-2019-12682, CVE-2019-12683, CVE-2019-12684, CVE-2019-12685, CVE-2019-12686, CVE-2019-12687, CVE-2019-12688, CVE-2019-12689, CVE-2019-12690, CVE-2019-12691, CVE-2019-12693, CVE-2019-12694, CVE-2019-12695, CVE-2019-12696, CVE-2019-12697, CVE-2019-12698, CVE-2019-12699, CVE-2019-12700, CVE-2019-12701, CVE-2019-12706, CVE-2019-12707, CVE-2019-12710, CVE-2019-12711, CVE-2019-12712, CVE-2019-12713, CVE-2019-12714, CVE-2019-12715, CVE-2019-12716, CVE-2019-15256, CVE-2019-15259, CVE-2019-15272, CVE-2019-1915

Zasiahnuté systémy

Cisco Security Manager
Cisco IC3000 Industrial Compute Gateway
Cisco Prime Infrastructure
Cisco Unified Contact Center Express
Cisco FXOS Software
Cisco Email Security Appliance
Cisco Adaptive Security Appliance (ASA)
Cisco Firepower
Cisco Unified Communications Manager
Cisco Unified Communications Manager Session Management Edition (SME)
Cisco Identity Services Engine (ISE)

Následky

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

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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-fmc-rce-12689
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-fmc-sql-inj
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-fxos-cmd-inject
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-ftd-fpmc-dos
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-ftd-container-esc
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-asa-ssl-vpn-dos
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-fmc-rce
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-asa-ospf-lsa-dos
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-fmc-com-inj
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-cucm-csrf
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-asa-ftd-sip-dos
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-asa-ftd-ikev1-dos
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-uccx-http
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-sm-java-deserial
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-asa-dos
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-pi-xss-12712
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-pi-xss-12713
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-ise-xss
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-ucm-secbypass
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-ic3000-icg-dos
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-ftd-cmdinj
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-firepwr-bypass
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-fmc-dir-trav
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-fire-bypass
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-esa-bypass
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-cucm-xss-12716
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-cucm-xxe
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-cuc-xss
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-cucm-xss-12715
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-cuc-inject
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-asa-xss
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-asa-scp-dos
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-asa-ftd-dos

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

Identifikátor

Apple iCloud a macOS zraniteľnosti

Popis

Spoločnosť Apple vydala bezpečnostné aktualizácie na svoje produkty macOS a iCloud, ktoré opravujú viacero bezpečnostných zraniteľností.
Najvážnejšie bezpečnostné zraniteľnosti umožňujú vzdialenému, autentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

07.10.2019

CVE

CVE-2019-11041, CVE-2019-11042, CVE-2019-8625, CVE-2019-8701, CVE-2019-8705, CVE-2019-8707, CVE-2019-8717, CVE-2019-8719, CVE-2019-8726, CVE-2019-8730, CVE-2019-8733, CVE-2019-8735, CVE-2019-8745, CVE-2019-8748, CVE-2019-8755, CVE-2019-8757, CVE-2019-8758, CVE-2019-8763, CVE-2019-8768, CVE-2019-8769, CVE-2019-8770, CVE-2019-8772, CVE-2019-8781

Zasiahnuté systémy

macOS verzie staršie ako Catalina 10.15
iCloud for Windows verzie staršie ako 7.14 a 10.7

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://support.apple.com/en-us/HT210634
https://support.apple.com/en-us/HT210636
https://support.apple.com/en-us/HT210637
https://www.theregister.co.uk/2019/10/07/apple_catalina_security/

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

Identifikátor

Zraniteľnosť produktov Yokogawa

Popis

Spoločnosť Yokogawa vydala bezpečnostné aktualizácie na portfólio svojich produktov, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

27.09.2019

CVE

CVE-2019-6008

Zasiahnuté systémy

Exaopc verzie staršie ako R3.78.00
Exaplog verzie staršie ako R3.40.00 a R3.40.06
Exaquantum verzie staršie ako R3.15.00
Exaquantum/Batchverzie staršie ako R3.10.00
Exasmoc (koniec podpory)
Exarqe (koniec podpory)
GA10 verzie staršie ako R3.05.06
InsightSuiteAE verzie staršie ako R1.07.00

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://web-material3.yokogawa.com/1/28032/files/YSAR-19-0003-E.pdf
https://www.us-cert.gov/ics/advisories/icsa-19-274-02

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

Identifikátor

Android zero-day zraniteľnosť

Popis

Bezpečnostní výskumníci informovali o bezpečnostnej zraniteľnosti v linuxovom jadre systému Android, ktorá je v súčasnosti aktívne zneužívaná útočníkmi.
Bezpečnostná zraniteľnosť v komponente Binder driver umožňuje vzdialenému, neautentifikovanému útočníkovi eskalovať svoje privilégiá na napadnutom systéme.

Dátum prvého zverejnenia varovania

04.10.2019

CVE

CVE-2019-2215

Zasiahnuté systémy

Android kernel okrem verzií 3.18, 4.4, a 4.9

Následky

Eskalácia privilégií

Odporúčania

Bezpečnostná aktualizácia opravujúca danú zraniteľnosť doposiaľ nebola vydaná. Odporúčame sledovať stránky výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a neinštalovali neoverené aplikácie.

Zdroje

https://bugs.chromium.org/p/project-zero/issues/detail?id=1942
https://thehackernews.com/2019/10/android-kernel-vulnerability.html
https://www.helpnetsecurity.com/2019/10/04/cve-2019-2215/
https://arstechnica.com/information-technology/2019/10/attackers-exploit-0day-vulnerability-that-gives-full-control-of-android-phones/

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.9
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

vBulletin zraniteľnosti

Popis

Vývojári systému vBulletin vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť vo funkcii ajax/api/user/updateAvatar je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi prostredníctvom zasielania špeciálne upravených požiadaviek vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

07.10.2019

CVE

CVE-2019-17132, CVE-2019-17271

Zasiahnuté systémy

vBulletin verzie staršie ako 5.5.4 Patch Level 2, 5.5.3, Patch Level 2 a 5.5.2 Patch Level 2

Následky

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

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://seclists.org/fulldisclosure/2019/Oct/8
https://seclists.org/fulldisclosure/2019/Oct/9
https://www.cybersecurity-help.cz/vdb/SB2019100801

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

Identifikátor

Ruby zraniteľnosti

Popis

Vývojári programovacieho jazyka Ruby vydali aktualizáciu svojho produktu, ktorá rieši viacero zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť v komponente lib/shell.rb je spôsobená nedostatočným overovaním používateľských vstupov a umožňuje lokálnemu, neautentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

01.10.2019

CVE

CVE-2019-15845, CVE-2019-16201, CVE-2019-16254, CVE-2019-16255

Zasiahnuté systémy

Ruby verzie staršie ako 2.4.8, 2.5.7 a 2.6.5

Následky

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

Odporúčania

Administrátorom zasiahnutých systémov odporúčame nainštalovať bezpečnostné aktualizácie.
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://www.ruby-lang.org/en/news/2019/10/01/ruby-2-6-5-released/
https://www.ruby-lang.org/en/news/2019/10/01/ruby-2-5-7-released/
https://www.ruby-lang.org/en/news/2019/10/01/ruby-2-4-8-released/
https://www.ruby-lang.org/en/news/2019/10/01/code-injection-shell-test-cve-2019-16255/
https://www.ruby-lang.org/en/news/2019/10/01/http-response-splitting-in-webrick-cve-2019-16254/
https://www.ruby-lang.org/en/news/2019/10/01/nul-injection-file-fnmatch-cve-2019-15845/
https://www.ruby-lang.org/en/news/2019/10/01/webrick-regexp-digestauth-dos-cve-2019-16201/
https://www.suse.com/security/cve/CVE-2019-16255/

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

Identifikátor

PuTTY zraniteľnosti

Popis

Vývojári PuTTY vydali bezpečnostnú aktualizáciu na svoj produkt, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

29.09.2019

CVE

CVE-2019-14961, CVE-2019-17067, CVE-2019-17069

Zasiahnuté systémy

PuTTY verzie staršie ako 0.73

Následky

Neoprávnený prístup k citlivým údajom
Zneprístupnenie služieb

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://lists.tartarus.org/pipermail/putty-announce/2019/000029.html

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

Identifikátor

Signal for Android zraniteľnosť

Popis

Vývojári komunikačnej aplikácie Signal vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť vo funkcii handleCallConnected umožňuje vzdialenému, neautentifikovanému útočníkovi zrealizovať audio hovor s používateľom bez toho, aby používateľ prichádzajúci hovor akceptoval.

Dátum prvého zverejnenia varovania

04.10.2019

CVE

-

Zasiahnuté systémy

Signal for Android verzie staršie ako v4.47.7

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://thehackernews.com/2019/10/signal-messenger-bug.html
https://bugs.chromium.org/p/project-zero/issues/detail?id=1943

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

Identifikátor

IBM Security Directory Server zraniteľnosti

Popis

Spoločnosť IBM vydala bezpečnostnú aktualizáciu na svoj produkt Security Directory Server, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi získať prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

01.10.2019

CVE

CVE-2019-4520, CVE-2019-4538, CVE-2019-4539, CVE-2019-4542, CVE-2019-4549

Zasiahnuté systémy

IBM Security Directory Server verzie staršie ako 6.4.0.19

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnený prístup do systému
Neoprávnená zmena v systéme

Odporúčania

Administrátorom odporúčame bezodkladne 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://www.ibm.com/support/pages/node/1077045

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.2
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Moxa EDR 810 zraniteľnosti

Popis

Spoločnosť Moxa vydala bezpečnostnú aktualizáciu na svoje smerovače rady EDR 810, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť vo webovej konzole je spôsobená nedostatočným overovaním používateľských vstupov a umožňuje vzdialenému, autentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

01.10.2019

CVE

CVE-2019-10963, CVE-2019-10969

Zasiahnuté systémy

Moxa EDR 810 verzie staršie ako 5.2

Následky

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

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://www.moxa.com/en/support/support/security-advisory/edr-810-series-secure-router-vulnerabilities-(1)
https://www.us-cert.gov/ics/advisories/icsa-19-274-03

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/SK-CERT-239