BEZPEČNOSTNÝ BULLETIN

Týždeň 24. 10. 2018 - 30. 10. 2018

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	X.Org X server zraniteľnosť	Vysoká	**8.8**
02.	Zraniteľnosti v ovládačoch ASRock	Vysoká	**8.4**
03.	Zraniteľnosti Advantech WebAccess	Vysoká	**8.4**
04.	Bezpečnostné zraniteľnosti v Apache Impala	Vysoká	**8.4**
05.	Bezpečnostná zraniteľnosti v Cisco Webex Meeting a Webex Productivity Tools	Vysoká	**7.8**
06.	Apache OFBiz XXE zraniteľnosť	Vysoká	**7.5**
07.	ProjeQtOr Zraniteľnosť	Vysoká	**7.3**
08.	Zraniteľnosť v systemd dhcp6	Vysoká	**7.3**
09.	Xen VT-x zraniteľnosť	Vysoká	**7.1**
10.	SQL injekcie v PHPTPoint Pharmacy Management System a Hospital Management System	Stredná	**6.5**
11.	SQL injekcie v SG ERP	Stredná	**6.5**
12.	BlueStacks App Player zraniteľnosť	Stredná	**6.3**
13.	GEOVAP Reliance 4 SCADA/HMI Zraniteľnosť	Stredná	**6.1**
14.	XSS zraniteľnosti v IBM Team Concert a IBM WebSphere Application Server	Stredná	**6.1**
15.	XSS zraniteľnosť v Citrix NetScaler Gateway	Stredná	**6.1**

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-170

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

Identifikátor

X.Org X server zraniteľnosť

Popis

Vývojári X.Org X serveru vydali bezpečnostnú aktualizáciu na svoj produkt, ktorá opravuje viacero bezpečnostných zraniteľností.
Najvážnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov v argumentoch -modulepath a -logfile a umožňuje vzdialenému autentifikovanému útočníkovi eskalovať svoje privilégiá a vykonať škodlivý kód na napadnutom systéme.

Dátum prvého zverejnenia varovania

25.10.2018

CVE

CVE-2018-14665

Zasiahnuté systémy

X.Org X server verzia 1.19

Následky

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

Odporúčania

Administrátorom zasiahnutých systémov odporúčame bezodkladne nainštalovať bezpečnostné aktualizácie.

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/151991
https://seclists.org/oss-sec/2018/q4/99

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

Identifikátor

Zraniteľnosti v ovládačoch ASRock

Popis

Spoločnosť Asrock vydala bezpečnostné aktualizáciu, ktoré opravujú viacero bezpečnostných zraniteľností v ovládačoch RGBLED, A-Tuning, F-Stream a RestartToUEFI.
Zraniteľnosti spočívajú v nedostatočnej implementácii mechanizmov riadenia prístupu k registrom v pamäti lokálny neautentifikovaný útočník by ich mohol zneužiť na vykonanie škodlivého kódu s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

25.01.2018

CVE

CVE-2018-10709, CVE-2018-10710, CVE-2018-10711, CVE-2018-10712

Zasiahnuté systémy

ASRock RGBLED verzie staršie ako 1.0.35.1
ASRock A-Tuning verzie staršie ako 3.0.210
ASRock F-Stream verzie staršie ako 3.0.210
ASRock RestartToUEFI verzie staršie ako 1.0.6.2

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/47
https://exchange.xforce.ibmcloud.com/vulnerabilities/152059
https://exchange.xforce.ibmcloud.com/vulnerabilities/152060
https://exchange.xforce.ibmcloud.com/vulnerabilities/152061
https://exchange.xforce.ibmcloud.com/vulnerabilities/152062

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

Identifikátor

Zraniteľnosti Advantech WebAccess

Popis

Spoločnosť Advantech vydala bezpečnostné aktualizácie, ktoré opravujú viacero zraniteľností v produkte WebAccess.
Prvá zraniteľnosť spočíva v nesprávnej konfigurácii mechanizmov riadenia prístupu počas inštalátorom a lokálny neautentifikovaný útočník by ju mohol zneužiť na vykonanie škodlivého kódu.
Druhá zraniteľnosť spočíva v nedostatočnom overovaní dĺžky používateľských vstupov a lokálny neautentifikovaný útočník by ju mohol zneužiť na vyvolanie pretečenia zásobníka a následné vykonanie škodlivého kódu.

Dátum prvého zverejnenia varovania

25.10.2018

CVE

CVE-2018-17908, CVE-2018-17910

Zasiahnuté systémy

Advantech WebAccess verzie 8.3.2 a staršie

Následky

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

Odporúčania

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

Zdroje

https://ics-cert.us-cert.gov/advisories/ICSA-18-298-02
https://exchange.xforce.ibmcloud.com/vulnerabilities/152022
https://exchange.xforce.ibmcloud.com/vulnerabilities/152023

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

Identifikátor

Bezpečnostné zraniteľnosti v Apache Impala

Popis

Spoločnosť Apache vydala bezpečnostné aktualizácie, ktoré opravujú viacero bezpečnostných zraniteľností v Apache Impala.
Najzávažnejšia zraniteľnosť v produkte Apache Impala spočíva v nesprávnej konfigurácii prístupových oprávnení k databáze a lokálny neautentifikovaný útočník by ju mohol zneužiť na eskaláciu privilégií v napadnutom systéme.
Druhá zraniteľnosť spočíva v nedostatočnej implementácii mechanizmov autentifikácie a vzdialený autentifikovaný útočník by ju mohol zneužiť na vykonanie neoprávnených zmien v systéme.

Dátum prvého zverejnenia varovania

24.10.2018

CVE

CVE-2018-11785, CVE-2018-11792

Zasiahnuté systémy

Apache Impala verzie staršie ako 3.0.1

Následky

Eskalácia privilégií, Neoprávnená zmena v systéme

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://seclists.org/oss-sec/2018/q4/97
https://exchange.xforce.ibmcloud.com/vulnerabilities/151974

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

Identifikátor

Bezpečnostná zraniteľnosti v Cisco Webex Meeting a Webex Productivity Tools

Popis

Spoločnosť Cisco vydala bezpečnostné aktualizácie, ktoré opravujú viacero bezpečnostných zraniteľností v produktoch Webex Meeting a Webex Productivity Tools.
Bezpečnostná zraniteľnosť v produkte Webex Meeting Desktop spočíva v nedostatočnom overovaní používateľských vstupov a lokálny autentifikovaný útočník by ju mohol zneužiť na vykonanie škodlivého kódu.

Dátum prvého zverejnenia varovania

24.10.2018

CVE

CVE-2018-15442

Zasiahnuté systémy

Cisco Webex Meetings Desktop App verzie staršie ako 33.5.6
Cisco Webex Productivity Tools verzie 32.6.0 až 33.0.5

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20181024-webex-injection
https://exchange.xforce.ibmcloud.com/vulnerabilities/151917

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

Identifikátor

Apache OFBiz XXE zraniteľnosť

Popis

Bezpečnostní výskumníci zverejnili informácie o bezpečnostnej zraniteľnosti v produkte Apache OFBiz. Zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a vzdialený neautentifikovaný útočník by ju prostredníctvom podvrhnutia špeciálne vytvorených požiadaviek mohol zneužiť na realizáciu XXE (XML External Entity) útoku a následné získanie prístupu k citlivým údajom.
Na uvedenú zraniteľnosť je v súčasnosti dostupný Proof-of-Concept kód.

Dátum prvého zverejnenia varovania

24.10.2018

CVE

-

Zasiahnuté systémy

Apache OFBiz verzie staršie ako 16.11.04

Následky

Neopravený prístup k citlivým údajom

Odporúčania

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

Zdroje

https://www.exploit-db.com/exploits/45673/
https://exchange.xforce.ibmcloud.com/vulnerabilities/151926

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.3**
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

ProjeQtOr Zraniteľnosť

Popis

Bezpečnostní výskumníci zverejnili informácie o bezpečnostnej zraniteľnosti v produkte ProjeQtOr slúžiacom na podporu manažmentu produktov.
Zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov v komponente nahrávania súborov a vzdialený autentifikovaný útočník by ju prostredníctvom podvrhnutia špeciálne vytvorených shtml súborov mohol zneužiť na vykonanie škodlivého kódu.
Na uvedenú zraniteľnosť je v súčasnosti dostupný Proof-of-Concept kód.

Dátum prvého zverejnenia varovania

25.10.2018

CVE

-

Zasiahnuté systémy

ProjeQtOr PMT verzie 7.2.5 a staršie

Následky

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

Odporúčania

Na uvedenú zraniteľnosť v súčasnosti nie sú dostupné bezpečnostné aktualizácie. Administrátorom a používateľom odporúčame sledovať stránky výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/151992

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.3
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Zraniteľnosť v systemd dhcp6

Popis

Vývojári systemd vydali bezpečnostnú aktualizáciu, ktorá opravuje bezpečnostnú zraniteľnosť v komponente dhcp6 client.
Zraniteľnosť by vzdialený neautentifikovaný útočník prostredníctvom podvrhnutia špeciálne vytvorených požiadaviek mohol zneužiť na vyvolanie pretečenia zásobníka a následné vykonanie škodlivého kódu.

Dátum prvého zverejnenia varovania

26.10.2018

CVE

CVE-2018-15688

Zasiahnuté systémy

systemd verzie 239 a staršie

Následky

Vykonanie škodlivého kódu

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/152041

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

Identifikátor

Xen VT-x zraniteľnosť

Popis

Vývojári produktu Xen vydali bezpečnostné aktualizácie na zraniteľnosť, ktorú by lokálny neautentifikovaný útočník mohol zneužiť na zneprístupnenie služby.
Uvedenú zraniteľnosť je možné zneužiť len na Intel x86 systémoch.

Dátum prvého zverejnenia varovania

24.10.2018

CVE

-

Zasiahnuté systémy

Xen verzie 4.9 a novšie

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

http://xenbits.xen.org/xsa/advisory-278.html
https://exchange.xforce.ibmcloud.com/vulnerabilities/151976

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

Identifikátor

SQL injekcie v PHPTPoint Pharmacy Management System a Hospital Management System

Popis

Bezpečnostní výskumníci informovali o bezpečnostných zraniteľnostiach v produktoch PHPTPoint Pharmacy Management System a PHPTPoint Hospital Management System.
Zraniteľnosti spočívajú v nedostatočnom overovaní používateľských vstupov a vzdialený neautentifikovaný útočník by ich mohol zneužiť na vykonanie SQL injekcie a následne zobraziť, pridať, upraviť alebo odstrániť údaje uložené v backend databáze.

Dátum prvého zverejnenia varovania

24.10.2018

CVE

CVE-2018-18704, CVE-2018-18705

Zasiahnuté systémy

PHPTPoint Pharmacy Management System verzie 1.0
PHPTPoint Hospital Management System verzie 1.0

Následky

Neoprávnený prístup do systému, Neoprávnená zmena v systéme

Odporúčania

Na uvedené zraniteľnosti v súčasnosti nie sú dostupné bezpečnostné aktualizácie. Odporúčame preveriť integritu databázy a prístupové logy na prítomnosť pokusov o SQL injekcie, sledovať stránky PHPTPoint a po vydaní bezpečnostných záplat vykonať aktualizáciu.

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/151982
https://exchange.xforce.ibmcloud.com/vulnerabilities/152009

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

Identifikátor

SQL injekcie v SG ERP

Popis

Bezpečnostní výskumníci zverejnili informácie o viacerých bezpečnostných zraniteľnostiach v produkte SG ERP.
Zraniteľnosti v valida_login.php a index.php by vzdialený neautentifikovaný útočník mohol zneužiť na vykonanie SQL injekcie a následne zobraziť, pridať, upraviť alebo odstrániť údaje uložené v backend databáze.

Dátum prvého zverejnenia varovania

24.10.2018

CVE

-

Zasiahnuté systémy

SG ERP verzie 1.0

Následky

Neoprávnená zmena v systéme

Odporúčania

Na uvedenú zraniteľnosť v súčasnosti nie sú dostupné bezpečnostné aktualizácie. Administrátorom odporúčame preveriť integritu databázy a prístupové logy na prítomnosť pokusov o SQL injekcie, sledovať stránky výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/151965

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

Identifikátor

BlueStacks App Player zraniteľnosť

Popis

Spoločnosť BlueStacks vydala bezpečnostné aktualizácie, ktoré opravujú zraniteľnosť v produkte Bluestack.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii mechanizmov riadenia prístupu a neautentifikovaný útočník v rovnakom sieťovom segmente by ju mohol zneužiť na získanie neoprávneného prístupu do systému.

Dátum prvého zverejnenia varovania

24.10.2018

CVE

CVE-2018-0701

Zasiahnuté systémy

BlueStacks App Player for Windows verzie 3.0.0 až 4.31.55
BlueStacks App Player for macOS verzie 2.0.0 a novšie

Následky

Neoprávnený prístup do systému

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov. Zneužitiu bezpečnostnej zraniteľnosti možno zabrániť aj prevádzkovaním BlueStacks inštalácií oddelene od Internetu alebo blokovaním prístupu z portu 5555/TCP.

Zdroje

https://support.bluestacks.com/hc/en-us/articles/360018274091
https://exchange.xforce.ibmcloud.com/vulnerabilities/151918

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 6.1
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

GEOVAP Reliance 4 SCADA/HMI Zraniteľnosť

Popis

Spoločnosť Geovap vydala bezpečnostnú aktualizáciu na svoj produkt Reliance 4 SCADA/HMI, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť umožňuje vzdialenému neautentifikovanému útočníkovi prostredníctvom útoku typu XSS (Cross-Site Scripting) vykonať škodlivý JavaScript kód.

Dátum prvého zverejnenia varovania

25.10.2018

CVE

CVE-2018-17904

Zasiahnuté systémy

Reliance SCADA 4 verzie staršie ako 4.8.0

Následky

Vykonanie škodlivého kódu

Odporúčania

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

Zdroje

https://ics-cert.us-cert.gov/advisories/ICSA-18-298-01
https://www.securityfocus.com/bid/105738/info

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 6.1
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

XSS zraniteľnosti v IBM Team Concert a IBM WebSphere Application Server

Popis

Spoločnosť IBM vydala bezpečnostné aktualizácie, ktoré opravujú viacero bezpečnostných zraniteľností v produktoch IBM Team Concert a IBM WebSphere Application Server.
Zraniteľnosti nachádzajúce sa v komponente Web UI spočívajú v nedostatočnom overovaní používateľských vstupov a vzdialený útočník by ju mohol zneužiť na realizáciu XSS (Cross-Site Scripting) útokov, vykonanie škodlivého kódu a získanie prístupu k citlivým údajom uloženým v cookies, vrátane autentifikačných údajov.

Dátum prvého zverejnenia varovania

25.10.2018

CVE

CVE-2018-1766, CVE-2018-1767

Zasiahnuté systémy

IBM Rational Collaborative Lifecycle Management verzie 5.0 až 6.0.5
IBM Rational Team Concert verzie 5.0 až 5.0.2
IBM Rational Team Concert verzie 6.0 až 6.0.5
IBM WebSphere Application verzie 7.0, 8.0, 8.5, 9.0, Liberty

Následky

Vykonanie škodlivého kódu, Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/148620
https://exchange.xforce.ibmcloud.com/vulnerabilities/148621

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 6.1
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

XSS zraniteľnosť v Citrix NetScaler Gateway

Popis

Spoločnosť Citrix vydala bezpečnostné aktualizácie, ktoré opravujú zraniteľnosť v produkte Citrix NetScaler Gateway.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a vzdialený neautentifikovaný útočník by ju prostredníctvom podvrhnutia špeciálne vytvorených URL mohol zneužiť na realizáciu XSS (Cross-Site Scripting) útokov, vykonanie škodlivého kódu a získanie prístupu k údajom uloženým v cookies, vrátane autentifikačných údajov.

Dátum prvého zverejnenia varovania

23.10.2018

CVE

CVE-2018-18517

Zasiahnuté systémy

Citrix NetScaler Gateway 10.5.x verzie staršie ako 10.5.69.3
Citrix NetScaler Gateway 11.1.x verzie staršie ako 11.1.59.10
Citrix NetScaler Gateway 12.0.x verzie staršie ako 12.0.58.18
Citrix NetScaler Gateway 12.1.x verzie staršie ako 12.1.49.23

Následky

Vykonanie škodlivého kódu, Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://support.citrix.com/article/CTX239002
https://exchange.xforce.ibmcloud.com/vulnerabilities/151978