BEZPEČNOSTNÝ BULLETIN

Týždeň 13. 02. 2019 - 19. 02. 2019

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Mozilla Firefox viacero zraniteľností	Vysoká	**8.8**
02.	Intel Data Center Manager SDK zraniteľnosti	Vysoká	**8.8**
03.	mIRC zraniteľnosť	Vysoká	**8.8**
04.	Raisecom GPON Devices zraniteľnosti	Vysoká	**8.6**
05.	SolarWinds Orion NPM	Vysoká	**8.1**
06.	Zraniteľnosť linuxového správcu balíčkov Snapd	Vysoká	**7.8**
07.	rssh zraniteľnosť	Vysoká	**7.8**
08.	Linux Kernel zraniteľnosť	Vysoká	**7.8**
09.	Cisco Network Assurance Engine zraniteľnosť	Vysoká	**7.7**
10.	Zraniteľnosť linuxového správcu balíčkov Flatpak	Vysoká	**7.7**
11.	EN100 Ethernet Communication Module a SIPROTEC5 relays zraniteľnosť	Vysoká	**7.5**
12.	Live Networks LIVE555 Media Server zraniteľnosti	Vysoká	**7.5**
13.	BIG-IP TMUI zraniteľnosť	Vysoká	**7.5**
14.	Pangea Communications Internet FAX ATA zraniteľnosť	Vysoká	**7.5**
15.	RVSiteBuilder CMS viacero zraniteľností	Vysoká	**7.5**
16.	IBM Rational ClearCase GIT connector zraniteľnosť	Vysoká	**7.5**
17.	Joomla! zraniteľnosti	Vysoká	**7.3**
18.	Mozilla Thunderbird viacero zraniteľností	Stredná	**6.5**

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:
01380/2019/TS/OKB-048

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

Identifikátor

Mozilla Firefox viacero zraniteľností

Popis

Spoločnosť Mozilla vydala bezpečnostné aktualizácie, ktoré opravujú viacero zraniteľností v internetových prehliadačoch Firefox a Firefox ESR.
Bezpečnostné zraniteľnosti sú spôsobené nedostatočným overovaním používateľských vstupov a umožňujú vzdialenému neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených súborov vykonať škodlivý kód.

Dátum prvého zverejnenia varovania

12.02.2019

CVE

CVE-2018-18356, CVE-2018-18511, CVE-2019-5785, CVE-2018-18335, CVE-2018-18356

Zasiahnuté systémy

Mozilla Firefox staršie ako 65.0.1
Mozilla Firefox ESR staršie ako 60.5.1

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.mozilla.org/en-US/security/advisories/mfsa2019-05/
https://www.mozilla.org/en-US/security/advisories/mfsa2019-04/

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

Identifikátor

Intel Data Center Manager SDK zraniteľnosti

Popis

Spoločnosť IBM vydala bezpečnostnú aktualizáciu na svoj produkt Data Center Manager SDK, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť vo webovom serveri je spôsobená nedostatočnou implementáciu bezpečnostných mechanizmov a umožňuje vzdialenému útočníkovi, nachádzajúcemu sa v rovnakom sieťovom segmente, eskalovať svoje privilégiá na napadnutom systéme.

Dátum prvého zverejnenia varovania

12.02.2019

CVE

CVE-2019-0102, CVE-2019-0103, CVE-2019-0104, CVE-2019-0105, CVE-2019-0106, CVE-2019-0107, CVE-2019-0108, CVE-2019-0109, CVE-2019-0110, CVE-2019-0111, CVE-2019-0112

Zasiahnuté systémy

Intel Data Center Manager SDK verzie staršie ako 5.0.2

Následky

Eskalácia privilégií
Neoprávnený prístup k citlivým údajom
Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.intel.com/content/www/us/en/security-center/advisory/INTEL-SA-00215.html

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

Identifikátor

mIRC zraniteľnosť

Popis

Vývojári komunikačného klienta mIRC vydali bezpečnostnú aktualizáciu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

18.02.2019

CVE

CVE-2019-6453

Zasiahnuté systémy

mIRC verzie staršie ako 7.55

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://proofofcalc.com/cve-2019-6453-mIRC/
https://proofofcalc.com/advisories/20190218.txt
https://nvd.nist.gov/vuln/detail/CVE-2019-6453

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 8.6
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Raisecom GPON Devices zraniteľnosti

Popis

Spoločnosť Raisecom vydala bezpečnostnú aktualizáciu na svoje GPON zariadenia, ktorá opravuje viacero bezpečnostných zraniteľností.
Bezpečnostné zraniteľnosti sú spôsobené nedostatočným overovaním používateľských vstupov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom podvrhnutia upravených špeciálne upravených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

12.02.2019

CVE

CVE-2019-7385, CVE-2019-7384

Zasiahnuté systémy

Raisecom ISCOM HT803G-U, HT803G-W, HT803G-1GE a HT803G GPON

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://seclists.org/fulldisclosure/2019/Feb/33
https://seclists.org/fulldisclosure/2019/Feb/34
https://exchange.xforce.ibmcloud.com/vulnerabilities/156954
https://exchange.xforce.ibmcloud.com/vulnerabilities/156955

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

Identifikátor

SolarWinds Orion NPM

Popis

Spoločnosť SolarWinds vydala bezpečnostnú aktualizáciu na svoj sieťový monitorovací systém Orion NPM, ktorá opravuje bezpečnostnú zraniteľnosť v komponente OrionModuleEngine.
Bezpečnostná zraniteľnosť je spôsobená nedostatočným overovaním používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne upravených požiadaviek vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

18.02.2019

CVE

CVE-2019-8917

Zasiahnuté systémy

SolarWinds Orion NPM verzie staršie ako 12.4

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://github.com/VerSprite/research/blob/master/advisories/VS-2019-001.md

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

Identifikátor

Zraniteľnosť linuxového správcu balíčkov Snapd

Popis

Vývojári linuxového správcu balíčkov Snapd vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť pomenovanú "Dirty_Sock".
Bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciu bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi eskalovať svoje privilégiá na napadnutom systéme.

Dátum prvého zverejnenia varovania

12.02.2019

CVE

CVE-2019-7304

Zasiahnuté systémy

Linuxové distribúcie využívajúce Snapd verzie staršie ako 2.37.1 (Ubuntu, Debian, Arch Linux, OpenSUSE, Solus, Fedora)

Následky

Eskalácia privilégií

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://shenaniganslabs.io/2019/02/13/Dirty-Sock.html
https://www.zdnet.com/article/dirty-sock-vulnerability-lets-attackers-gain-root-access-on-linux-systems/
https://usn.ubuntu.com/3887-1/
https://exchange.xforce.ibmcloud.com/vulnerabilities/156939
https://tools.cisco.com/security/center/viewAlert.x?alertId=59642

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

Identifikátor

rssh zraniteľnosť

Popis

Vývojári rssh vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciu bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi vykonať škodlivý kód.

Dátum prvého zverejnenia varovania

30.01.2019

CVE

CVE-2019-1000018

Zasiahnuté systémy

Linuxové distribúcie využívajúce rssh verzie staršie ako 2.3.4-4+deb8u1

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://esnet-security.github.io/vulnerabilities/20190115_rssh
https://nvd.nist.gov/vuln/detail/CVE-2019-1000018

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

Identifikátor

Linux Kernel zraniteľnosť

Popis

Vývojári linuxového jadra vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť v kvm_ioctl_create_device funkcii.
Bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi eskalovať svoje privilégiá na napadnutom systéme.

Dátum prvého zverejnenia varovania

07.02.2019

CVE

CVE-2019-6974

Zasiahnuté systémy

Linux Kernel verzie staršie ako 4.20.8

Následky

Eskalácia privilégií
Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://tools.cisco.com/security/center/viewAlert.x?alertId=59645
https://access.redhat.com/security/cve/cve-2019-6974
https://git.kernel.org/pub/scm/virt/kvm/kvm.git/commit/?id=cfa39381173d5f969daf43582c95ad679189cbc9

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.7**
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Cisco Network Assurance Engine zraniteľnosť

Popis

Spoločnosť Cisco vydala bezpečnostnú aktualizáciu na svoj produkt Cisco Network Assurance Engine, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi získať neoprávnený prístup do systému a spôsobiť zneprístupnenie služieb.

Dátum prvého zverejnenia varovania

12.02.2019

CVE

CVE-2019-1688

Zasiahnuté systémy

Cisco Network Assurance Engine (NAE) Release 3.0(1)

Následky

Neoprávnený prístup do systému
Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190212-nae-dos

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.7**
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Zraniteľnosť linuxového správcu balíčkov Flatpak

Popis

Vývojári správcu balíčkov Flatpak vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi eskalovať svoje privilégiá na zraniteľnom systéme.

Dátum prvého zverejnenia varovania

10.02.2019

CVE

CVE-2019-8308

Zasiahnuté systémy

Flatpak verzie staršie ako 1.0.7 a 1.2.3

Následky

Eskalácia privilégií

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://tools.cisco.com/security/center/viewAlert.x?alertId=59639

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

Identifikátor

EN100 Ethernet Communication Module a SIPROTEC5 relays zraniteľnosť

Popis

Spoločnosť Siemens vydala bezpečnostné aktualizácie na svoje produkty EN100 a SIPROTEC5, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená spôsobená nedostatočnou implementáciu bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania paketov na port 102/TCP spôsobiť zneprístupnenie služieb.

Dátum prvého zverejnenia varovania

12.02.2019

CVE

CVE-2018-16563

Zasiahnuté systémy

SIPROTEC 5 verzie staršie ako 7.82 a 7.58
EN100 Ethernet module IEC 61850 verzie staršie ako 4.35

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov. Tiež odporúčame aplikovať firewallové pravidlá a blokovať TCP port 102.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

https://cert-portal.siemens.com/productcert/pdf/ssa-104088.pdf

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

Identifikátor

Live Networks LIVE555 Media Server zraniteľnosti

Popis

Bezpečnostní výskumníci informovali o bezpečnostných zraniteľnostiach v produkte Live Networks LIVE555 Media Server. Bezpečnostné zraniteľnosti sú spôsobené nedostatočným overovaním používateľských vstupov a umožňujú vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania HTTP paketov spôsobiť zneprístupnenie služieb na zasiahnutom systéme.

Dátum prvého zverejnenia varovania

11.02.2019

CVE

CVE-2019-7733, CVE-2019-7732

Zasiahnuté systémy

Live Networks LIVE555 Media Server

Následky

Zneprístupnenie služby

Odporúčania

Bezpečnostné aktualizácie doposiaľ neboli vydané. Odporúčame sledovať stránky výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu.

Zdroje

https://tools.cisco.com/security/center/viewAlert.x?alertId=59608
https://tools.cisco.com/security/center/viewAlert.x?alertId=59607
https://github.com/rgaufman/live555/issues/21
https://github.com/rgaufman/live555/issues/20

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

Identifikátor

BIG-IP TMUI zraniteľnosť

Popis

Spoločnosť F5 vydala bezpečnostnú aktualizáciu na svoj produkt BIG-IP, ktorá opravuje bezpečnostnú zraniteľnosť v Traffic Management User Interface.
Bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia upravených URL adries vykonať škodlivý kód.

Dátum prvého zverejnenia varovania

29.01.2019

CVE

CVE-2019-6589

Zasiahnuté systémy

BIG-IP verzie staršie ako 14.1.0, 14.0.0.3, 13.1.1.4, 12.1.4, 11.6.3.3

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://support.f5.com/csp/article/K23566124

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

Identifikátor

Pangea Communications Internet FAX ATA zraniteľnosť

Popis

Spoločnosť Pangea Communications vydala bezpečnostnú aktualizáciu na svoj produkt Internet FAX ATA, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nedostatočným overovaním používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia upravených URL adries spôsobiť pád systému a zneprístupnenie služieb.

Dátum prvého zverejnenia varovania

14.02.2019

CVE

CVE-2019-6551

Zasiahnuté systémy

Pangea Communications Internet FAX ATA verzie 3.1.8 a staršie

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://ics-cert.us-cert.gov/advisories/ICSA-19-045-01

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

Identifikátor

RVSiteBuilder CMS viacero zraniteľností

Popis

Bezpečnostní výskumníci informovali o bezpečnostných zraniteľnostiach v redakčnom systéme RVSiteBuilder. Najzávažnejšie bezpečnostné zraniteľnosti sú spôsobené nedostatočnou implementáciu bezpečnostných mechanizmov a umožňujú vzdialenému, neautentifikovanému útočníkovi získať prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

14.02.2019

CVE

-

Zasiahnuté systémy

RVSiteBuilder CMS verzia 7.0 a staršie

Následky

Neoprávnená zmena v systéme
Neoprávnený prístup k citlivým údajom

Odporúčania

Spoločnosť RVGlobalSoft doposiaľ nevydala bezpečnostnú aktualizáciu. Odporúčame sledovať stránky výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu.

Zdroje

https://packetstormsecurity.com/files/151675
https://exchange.xforce.ibmcloud.com/vulnerabilities/157061

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

Identifikátor

IBM Rational ClearCase GIT connector zraniteľnosť

Popis

Spoločnosť IBM vydala bezpečnostnú aktualizáciu na svoj produkt Rational ClearCase, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciu bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup k dokumentom v databáze.

Dátum prvého zverejnenia varovania

12.02.2019

CVE

CVE-2019-4059

Zasiahnuté systémy

IBM Rational ClearCase GIT connector verzie staršie ako 1.0.0.1

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www-01.ibm.com/support/docview.wss?uid=ibm10870810
https://exchange.xforce.ibmcloud.com/vulnerabilities/156583

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

Identifikátor

Joomla! zraniteľnosti

Popis

Vývojári systému pre správu obsahu Joomla! vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť v komponente phar:// stream wrapper umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne upravených požiadaviek vykonať škodlivý kód.

Dátum prvého zverejnenia varovania

12.02.2019

CVE

CVE-2019-6261, CVE-2019-6262, CVE-2019-6263, CVE-2019-6264, CVE-2019-7739, CVE-2019-7740, CVE-2019-7741, CVE-2019-7742, CVE-2019-7743, CVE-2019-7744

Zasiahnuté systémy

Joomla! CMS vezrie staršie ako 3.9.2

Následky

Vykonanie škodlivého kódu
Neoprávnený prístup k citlivým údajom

Odporúčania

Odporúčame uistiť sa, či Vaše webové stránky nie sú založené na redakčnom systéme Joomla! v zraniteľnej verzii. V prípade že áno, zabezpečte aktualizáciu redakčného systému.

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/156907
https://developer.joomla.org/security-centre/770-20190206-core-implement-the-typo3-phar-stream-wrapper
https://exchange.xforce.ibmcloud.com/vulnerabilities/156906
https://developer.joomla.org/security-centre/766-20190202-core-browserside-mime-type-sniffing-causes-xss-attack-vectors
https://exchange.xforce.ibmcloud.com/vulnerabilities/156905
https://developer.joomla.org/security-centre/768-20190204-core-stored-xss-issue-in-the-global-configuration-help-url-2
https://exchange.xforce.ibmcloud.com/vulnerabilities/156904
https://developer.joomla.org/security-centre/769-20190205-core-xss-issue-in-core-js-writedynalist
https://exchange.xforce.ibmcloud.com/vulnerabilities/156902
https://developer.joomla.org/security-centre/767-20190203-core-additional-warning-in-the-global-configuration-textfilter-settings
https://exchange.xforce.ibmcloud.com/vulnerabilities/156908
https://developer.joomla.org/security-centre/765-20190201-core-lack-of-url-filtering-in-various-core-components

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/TS/OKB-048

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

Identifikátor

Mozilla Thunderbird viacero zraniteľností

Popis

Spoločnosť Mozilla vydala bezpečnostnú aktualizáciu, ktorá opravuje viacero zraniteľností v e-mailovom klientovi Thunderbird.
Bezpečnostné zraniteľnosti sú spôsobené nedostatočným overovaním používateľských vstupov a umožňujú vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených súborov spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

14.02.2019

CVE

CVE-2018-18335, CVE-2018-18356, CVE-2018-18509, CVE-2019-5785

Zasiahnuté systémy

Mozilla Thunderbird verzie staršie ako 60.5.1

Následky

Zneprístupnenie služby
Neoprávnený prístup k citlivým údajom

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.mozilla.org/en-US/security/advisories/mfsa2019-06/

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/TS/OKB-048