BEZPEČNOSTNÝ BULLETIN

Týždeň 22. 05. 2019 - 28. 05. 2019

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Artifex Ghostscript zraniteľnosť	Vysoká	**8.8**
02.	Computrols CBAS Web zraniteľnosť	Vysoká	**8.8**
03.	Mozilla Firefox zraniteľnosti	Vysoká	**8.8**
04.	Oracle Solaris zraniteľnosť	Vysoká	**7.8**
05.	FreeImage zraniteľnosti	Vysoká	**7.5**
06.	FasterXML Jackson zraniteľnosť	Vysoká	**7.5**
07.	Mitsubishi Electric MELSEC-Q Series zraniteľnosť	Vysoká	**7.5**
08.	Jenkins viacero zraniteľností	Stredná	**6.8**
09.	Joomla! zraniteľnosti	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:
01380/2019/TS/OKB-143

BEZPEČNOSTNÝ BULLETIN

Týždeň 22. 05. 2019 - 28. 05. 2019

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

Identifikátor

Artifex Ghostscript zraniteľnosť

Popis

Spoločnosť Artifex vydala bezpečnostnú aktualizáciu na svoj produkt Ghostscript. Zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvoreného PostScript súboru získať neoprávnený prístup do systému.

Dátum prvého zverejnenia varovania

23.05.2019

CVE

CVE-2019-3839

Zasiahnuté systémy

Artifex Ghostscript verzie staršie ako 9.28

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnený prístup do 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.
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://tools.cisco.com/security/center/viewAlert.x?alertId=60215
http://git.ghostscript.com/?p=ghostpdl.git&a=patch&h=db24f253409d5d085c2760c814c3e1d3fa2dac59

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

Identifikátor

Computrols CBAS Web zraniteľnosť

Popis

Spoločnosť Computrols vydala bezpečnostné aktualizácie na svoj produkt CBAS Web, ktoré opravujú viacero bezpečnostných zraniteľností. Najzávažnejšia zraniteľnosť umožňuje vzdialenému, autentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

21.05.2019

CVE

CVE-2019-10846, CVE-2019-10847, CVE-2019-10848, CVE-2019-10849, CVE-2019-10851, CVE-2019-10852, CVE-2019-10853, CVE-2019-10854, CVE-2019-10855

Zasiahnuté systémy

Computrols CBAS Web verzie staršie ako 19.0.1
Computrols CBAS Web verzie staršie ako 18.0.1
Computrols CBAS Web verzie staršie ako 15.0.1
Computrols CBAS Web verzie staršie ako 14.0.1
Computrols CBAS Web verzie staršie ako 8.0.7
Computrols CBAS Web verzie staršie ako 7.2.1-Beta
Computrols CBAS Web verzie staršie ako 6.9.2
Computrols CBAS Web verzie staršie ako 4.8.2
Computrols CBAS Web verzie staršie ako 3.15.1

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.
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://ics-cert.us-cert.gov/advisories/ICSA-19-141-01
http://www.computrols.com/wp-content/uploads/2019/05/CBAS-Web-Advisory-2019-5-9.pdf

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

Identifikátor

Mozilla Firefox zraniteľnosti

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

21.05.2019

CVE

CVE-2018-18511, CVE-2019-11691, CVE-2019-11692, CVE-2019-11693, CVE-2019-11694, CVE-2019-11695, CVE-2019-11696, CVE-2019-11697, CVE-2019-11698, CVE-2019-11699, CVE-2019-11700, CVE-2019-11701, CVE-2019-5798, CVE-2019-7317, CVE-2019-9797, CVE-2019-9800, CVE-2019-9814, CVE-2019-9815, CVE-2019-9816, CVE-2019-9817, CVE-2019-9818, CVE-2019-9819, CVE-2019-9820, CVE-2019-9821

Zasiahnuté systémy

Mozilla Firefox verzie staršie ako 67
Firefox ESR verzie staršie ako 60.7

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.
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/mfsa2019-13/
https://www.mozilla.org/en-US/security/advisories/mfsa2019-14/

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

Identifikátor

Oracle Solaris zraniteľnosť

Popis

Bezpečnostní výskumníci zverejnili bezpečnostnú zraniteľnosť v operačnom systéme Oracle Solaris v module dtprintinfo.
Zraniteľnosť je spôsobená nedostatočným overovaním používateľských vstupov a umožňuje lokálnemu, autentifikovanému útočníkovi eskalovať svoje privilégiá.

Dátum prvého zverejnenia varovania

20.05.2019

CVE

-

Zasiahnuté systémy

Oracle Solaris 7
Oracle Solaris 8
Oracle Solaris 9
Oracle Solaris 10

Následky

Eskalácia privilégií

Odporúčania

Administrátorom odporúčame sledovať stránky výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu.

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/161277
https://packetstormsecurity.com/files/152970
https://www.exploit-db.com/exploits/46877

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

Identifikátor

FreeImage zraniteľnosti

Popis

Bezpečnostní výskumníci informovali o bezpečnostných zraniteľnostiach v produkte FreeImage. Najzávažnejšia bezpečnostná zraniteľnosť je spôsobená nedostatočným overovaním používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom špeciálne vytvorených súborov spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

24.05.2019

CVE

CVE-2019-12212, CVE-2019-12213, CVE-2019-12214

Zasiahnuté systémy

FreeImage verzie 3.18 a staršie

Následky

Zneprístupnenie služby

Odporúčania

Odporúčame uistiť sa, či Vaše aplikácie a produkty nevyužívajú FreeImage. V prípade, že áno, 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 nenavštevovali nedôveryhodné webové stránky.

Zdroje

https://tools.cisco.com/security/center/viewAlert.x?alertId=60220
https://tools.cisco.com/security/center/viewAlert.x?alertId=60219
https://tools.cisco.com/security/center/viewAlert.x?alertId=60218
https://sourceforge.net/p/freeimage/discussion/36111/thread/e06734bed5/

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

Identifikátor

FasterXML Jackson zraniteľnosť

Popis

Vývojári FasterXML Jackson vydali bezpečnostnú aktualizáciu, ktorá opravuje bezpečnostnú zraniteľnosť. Bezpečnostná zraniteľnosť v komponente jackson-databind je spôsobená nedostatočným overovaním používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvoreného JSON súboru získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

23.05.2019

CVE

CVE-2019-12086

Zasiahnuté systémy

FasterXML jackson-databind verzie staršie ako 2.9.9

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Odporúčame uistiť sa, či Vaše aplikácie a produkty nevyužívajú FasterXML. V prípade že áno, 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://tools.cisco.com/security/center/viewAlert.x?alertId=60213
https://github.com/FasterXML/jackson-databind/issues/2326
https://github.com/FasterXML/jackson-databind/releases

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

Identifikátor

Mitsubishi Electric MELSEC-Q Series zraniteľnosť

Popis

Spoločnosť Mitsubishi Electric vydala bezpečnostnú aktualizáciu na svoje produkty MELSEC-Q, ktorá opravuje bezpečnostnú zraniteľnosť v FTP komponente. Zraniteľnosť umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania TCP paketov spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

21.05.2019

CVE

CVE-2019-10977

Zasiahnuté systémy

MELSEC-Q series Ethernet module verzie QJ71E71-100 so sériovým číslom starším ako 20121

Následky

Zneprístupnenie služby

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-19-141-02
https://us.mitsubishielectric.com/fa/en/about-us/distributors

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 6.8
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Jenkins viacero zraniteľností

Popis

Vývojári produktu Jenkins vydali bezpečnostné aktualizácie na zásuvné moduly, ktoré opravujú viacero bezpečnostných zraniteľností. Najzávažnejšia bezpečnostná zraniteľnosť v Jenkins GitHub Authentication Plugin je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

30.04.2019

CVE

CVE-2019-10307, CVE-2019-10308, CVE-2019-10309, CVE-2019-10310, CVE-2019-10311, CVE-2019-10312, CVE-2019-10313, CVE-2019-10314, CVE-2019-10315, CVE-2019-10316, CVE-2019-10317, CVE-2019-10318

Zasiahnuté systémy

Jenkins Ansible Tower verzie staršie ako 0.9.2
Jenkins Static Analysis Utilities verzie staršie ako 1.96
Jenkins Twitter verzia 0.7
Jenkins Aqua Microscanner verzie staršie ako 1.0.6
Jenkins Sitemonitor verzie staršie ako 0.6
Jenkins Self-organizing Swarm Modules
Jenkins Koji verzia 0.3
Jenkins Github Authentication verzie staršie ako 0.32
Jenkins Azure AS verzie staršie ako 0.3.4

Následky

Neoprávnený prístup k citlivým údajom

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://jenkins.io/security/advisory/2019-04-30/
https://www.cvedetails.com/cve/CVE-2019-10315/
https://nvd.nist.gov/vuln/detail/CVE-2019-10315

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

Identifikátor

Joomla! zraniteľnosti

Popis

Vývojári systému pre správu obsahu Joomla! vydali bezpečnostnú aktualizáciu na svoj produkt, ktorá opravuje bezpečnostné zraniteľnosti. Zraniteľnosti spočívajú v nedostatočnom overovaní používateľských vstupov a umožňujú vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

23.05.2019

CVE

CVE-2019-11809

Zasiahnuté systémy

Joomla! verzie staršie ako 3.9.6

Následky

Neoprávnený prístup k citlivým údajom

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.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.

Zdroje

https://tools.cisco.com/security/center/viewAlert.x?alertId=60214
https://www.joomla.org/announcements/release-news/5765-joomla-3-9-6-release.html
https://developer.joomla.org/security-centre/781-%2020190502-core-by-passing-protection-of-phar-stream-wrapper-interceptor.html
https://developer.joomla.org/security-centre/780-20190501-core-xss-in-com-users-acl-debug-view

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-143