BEZPEČNOSTNÝ BULLETIN

Týždeň 20. 02. 2019 - 26. 02. 2019

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Zraniteľnosti produktov Cisco	Vysoká	**8.8**
02.	Zraniteľnosti produktov Xerox	Vysoká	**8.8**
03.	Bosh Smart Camera App for Android zraniteľnosti	Vysoká	**8.3**
04.	Horner Automation Cscape zraniteľnosť	Vysoká	**7.8**
05.	LG Device Manager application zraniteľnosť	Vysoká	**7.8**
06.	Filr zraniteľnosti	Vysoká	**7.8**
07.	Zraniteľnosť v Adobe Acrobat a Reader	Vysoká	**7.5**
08.	BIND zraniteľnosť	Vysoká	**7.5**
09.	Splunk Web XSS zraniteľnosť	Vysoká	**7.4**

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-053

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

Identifikátor

Zraniteľnosti produktov Cisco

Popis

Spoločnosť Cisco vydala bezpečnostné aktualizácie na väčšie množstvo svojich produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť v Cisco HyperFlex Software je spôsobená nedostatočným overovaním používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.
Zraniteľnosť v komponente Quality of Voice Reporting produktu Cisco Prime Collaboration Assurance spočíva v nedostatočnej implementácii autentifikačných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup do systému.

Dátum prvého zverejnenia varovania

20.02.2019

CVE

CVE-2019-1685, CVE-2019-1684, CVE-2019-1700, CVE-2019-1691, CVE-2019-1666, CVE-2019-1667, CVE-2019-1665, CVE-2019-1698, CVE-2019-1683, CVE-2019-1689, CVE-2019-1680, CVE-2019-1664, CVE-2018-15380, CVE-2019-1681, CVE-2019-1662, CVE-2019-1659

Zasiahnuté systémy

Cisco HyperFlex Software verzie staršie ako 3.5(2a)
Cisco Prime Infrastructure Software Releases 2.2 až 3.4.0
Cisco PCA Software verzie staršie ako 12.1 SP2
Cisco IOS XR Software verzie staršie ako 6.5.2
Cisco Webex Meetings Online (meetings.webex.com) verzie staršie ako 1.3.42
Cisco SPA112, Cisco SPA525, a Cisco SPA5x5 Series IP Phones
Cisco IoT-FND Software
Cisco Firepower Threat Defense Software
Cisco Firepower 9000 Series with PID FPR9K-DNM-2X100G
Cisco Unity Connection
Cisco IP Phone 7800 and 8800 Series

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému
Zneprístupnenie služby
Neoprávnený prístup do 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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190220-prime-validation
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190220-pca-access
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190220-ncs
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190220-hyperflex-injection
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190220-chn-root-access
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190206-webex-injection
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190220-webx-ios-file
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190220-ipphone-certs
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190220-cuc-rxss
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190220-cdp-lldp-dos
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190220-firpwr-dos
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190220-fpwr-ssltls-dos
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190220-hyper-retrieve
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190220-hyper-write
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190220-hyper-xss
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190220-iot-fnd-xml

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

Identifikátor

Zraniteľnosti produktov Xerox

Popis

Spoločnosť Xerox vydala bezpečnostné aktualizácie na viaceré svoje produkty, ktoré opravujú väčšie množstvo bezpečnostných zraniteľností.
Najzávažnejšie bezpečnostné zraniteľnosti umožňujú vzdialenému, autentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

20.02.2019

CVE

CVE-2011-0465, CVE-2011-0997, CVE-2017-12176, CVE-2017-12177, CVE-2017-12178, CVE-2017-12179, CVE-2017-12180, CVE-2017-12181, CVE-2017-12182, CVE-2017-12183, CVE-2017-12184, CVE-2017-12185, CVE-2017-12186, CVE-2017-12187, CVE-2018-0732, CVE-2018-0734, CVE-2018-0735, CVE-2018-0737, CVE-2018-5407, CVE-2018-5740, CVE-2018-8653, CVE-2019-0536, CVE-2019-0538, CVE-2019-0541, CVE-2019-0543, CVE-2019-0545, CVE-2019-0549, CVE-2019-0554, CVE-2019-0569, CVE-2019-0575, CVE-2019-0576, CVE-2019-0577, CVE-2019-0578, CVE-2019-0579, CVE-2019-0580, CVE-2019-0581, CVE-2019-0582, CVE-2019-0583, CVE-2019-0584, CVE-2019-2541, CVE-2019-2543, CVE-2019-2544

Zasiahnuté systémy

Xerox Color 800i/1000i Press
Xerox Versant3100 Press
Xerox FreeFlow Print Server v2 (Xerox Color C60/C70, Xerox iGen 5 Press, Xerox BrenvaHD Production InkJet Printer Products)
Xerox FreeFlow Print Server v7 (Xerox Nuvera PSIP 14.0 Printer Products)
Xerox FreeFlow Print Server v8 (Solaris 10 OS)
Xerox FreeFlow Print Server v9 (Solaris 10 OS)

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov, aplikovať firewallové pravidlá a limitovať prístup k zasiahnutým zariadeniam z 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://security.business.xerox.com/wp-content/uploads/2019/02/cert_XRX19-005_FFPSv2_Win7_SecurityBulletin_Feb2019.pdf https://security.business.xerox.com/wp-content/uploads/2019/02/cert_XRX19-004_FFPSv7-S11_MediaDelivery_Feb2019.pdf https://security.business.xerox.com/wp-content/uploads/2019/02/cert_XRX19-003_FFPSv9-S10_DvdUsb_Feb2019.pdf https://security.business.xerox.com/wp-content/uploads/2019/02/cert_XRX19-002_FFPSv8-S10_DvdUsb_Feb2019.pdf https://security.business.xerox.com/wp-content/uploads/2019/02/cert_XRX19-001_FFPSv7-S10_DvdUsb_Feb2019.pdf https://security.business.xerox.com/wp-content/uploads/2019/02/cert_XRX19-006_FFPSv9-S11_MediaDelivery_Feb2019.pdf

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.3**
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Bosh Smart Camera App for Android zraniteľnosti

Popis

Spoločnosť Bosh vydala bezpečnostnú aktualizáciu na svoj produkt Smart Camera App, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť je spôsobená nedostatočným overovaním bezpečnostných TLS certifikátov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom prostredníctvom man-in-the-middle útoku získať neoprávnený prístup do systému.

Dátum prvého zverejnenia varovania

14.02.2019

CVE

CVE-2019-7728, CVE-2019-7729

Zasiahnuté systémy

Bosh Smart Camera App for Android verzie staršie ako 1.3.1

Následky

Neoprávnený prístup do systému
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://psirt.bosch.com/Advisory/BOSCH-2019-0202.html
https://psirt.bosch.com/Advisory/BOSCH-2019-0204.html

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

Identifikátor

Horner Automation Cscape zraniteľnosť

Popis

Spoločnosť Horner Automation vydala bezpečnostnú aktualizáciu na svoj produkt Cscape, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nedostatočným overovaním používateľských vstupov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených POC súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

19.02.2019

CVE

CVE-2019-6555

Zasiahnuté systémy

Cscape verzie staršie ako 9.90

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://ics-cert.us-cert.gov/advisories/ICSA-19-050-03

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

Identifikátor

LG Device Manager application zraniteľnosť

Popis

Spoločnosť LG vydala bezpečnostnú aktualizáciu na svoj produkt LG Device Manager application, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi eskalovať svoje privilégiá na napadnutom systéme.

Dátum prvého zverejnenia varovania

17.02.2019

CVE

CVE-2019-8372

Zasiahnuté systémy

LG Device Manager application v LG notebookoch verzie T350, 10T370, 15U560, 15UD560, 14Z960, 14ZD960, 15Z960, 15ZD960 a tiež notebookoch so Skylake procesormi

Následky

Eskalácia privilégií

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

http://www.jackson-t.ca/lg-driver-lpe.html
https://securityaffairs.co/wordpress/81323/hacking/lg-device-manager-flaw.html

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

Identifikátor

Filr zraniteľnosti

Popis

Spoločnosť Micro Focus vydala bezpečnostnú aktualizáciu na svoj produkt Filr, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť v komponente famtd umožňuje lokálnemu, autentifikovanému útočníkovi eskalovať svoje privilégiá na napadnutom systéme.

Dátum prvého zverejnenia varovania

19.02.2019

CVE

CVE-2019-3474, CVE-2019-3475

Zasiahnuté systémy

Micro Focus Filr 3.0 verzie staršie ako Security Update 6

Následky

Eskalácia privilégií
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://support.microfocus.com/kb/doc.php?id=7023727
https://support.microfocus.com/kb/doc.php?id=7023726
https://www.secureauth.com/labs/advisories/micro-focus-filr-multiple-vulnerabilities

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

Identifikátor

Zraniteľnosť v Adobe Acrobat a Reader

Popis

Spoločnosť Adobe vydala bezpečnostné aktualizácie na svoje produkty Adobe Acrobat a Reader, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

21.02.2019

CVE

CVE-2019-7815

Zasiahnuté systémy

Adobe Acrobat a Reader verzie staršie ako 2019.010.20098, 2017.011.30127 a 2015.006.30482

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://helpx.adobe.com/security/products/acrobat/apsb19-13.html
https://www.securityweek.com/adobe-releases-second-patch-data-leakage-flaw-reader
https://www.tenable.com/plugins/nessus/122366

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

Identifikátor

BIND zraniteľnosť

Popis

Vývojári DNS servera BIND vydali bezpečnostné aktualizácie svojho produktu, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne upravených paketov spôsobiť zneprístupnenie služieb a únik údajov z pamäti procesu.

Dátum prvého zverejnenia varovania

21.02.2019

CVE

CVE-2018-5744, CVE-2018-5745, CVE-2019-6465

Zasiahnuté systémy

BIND verzie staršie ako 9.11.5-P4,9.11.5-S5 a 9.12.3-P4

Následky

Zneprístupnenie služby
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://kb.isc.org/docs/cve-2018-5744
https://kb.isc.org/docs/cve-2018-5745
https://kb.isc.org/docs/cve-2019-6465
https://tools.cisco.com/security/center/viewAlert.x?alertId=59675
https://exchange.xforce.ibmcloud.com/vulnerabilities/157371

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.4**
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Splunk Web XSS zraniteľnosť

Popis

Spoločnosť Splunk vydala bezpečnostnú aktualizáciu na svoj produkt Splunk Web, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nedostatočným overovaním používateľských vstupov 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

19.02.2019

CVE

CVE-2019-5727

Zasiahnuté systémy

Splunk Enterprise verzie staršie ako 6.5.5, 6.4.9, 6.3.12, 6.2.14, 6.1.14, 6.0.15 a Splunk Light verzie staršie ako 6.6.0

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.splunk.com/view/SP-CAAAQAF
https://tools.cisco.com/security/center/viewAlert.x?alertId=59670