BEZPEČNOSTNÝ BULLETIN

Týždeň 23. 01. 2019 - 29. 01. 2019

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Phoenix Contact FL Switch zraniteľnosti	Vysoká	**8.8**
02.	Microsoft Exchange NTLM zraniteľnosť	Vysoká	**8.8**
03.	Foxit PhantomPDF zraniteľnosti	Vysoká	**8.8**
04.	Cisco Firepower Threat Defense zraniteľnosť	Vysoká	**8.6**
05.	Dräger Infinity Delta zraniteľnosti	Vysoká	**8.4**
06.	Cisco Webex Teams client zraniteľnosť	Vysoká	**7.8**
07.	Cisco Webex Player zraniteľnosti	Vysoká	**7.8**
08.	Artifex Software Ghostscript zraniteľnosť	Vysoká	**7.8**
09.	Apache HTTP Server zraniteľnosť	Vysoká	**7.5**
10.	Cisco IoT Field Network Director zraniteľnosť	Vysoká	**7.5**
11.	LabKey Server viacero zraniteľností	Vysoká	**7.5**
12.	phpMyAdmin zraniteľnosti	Vysoká	**7.5**
13.	Johnson Controls Facility Explorer zraniteľnosti	Vysoká	**7.4**
14.	Jenkins cookies zraniteľnosti	Vysoká	**7.2**
15.	Cisco Identity Services Engine zraniteľnosť	Stredná	**6.5**
16.	7-Zip zraniteľnosť šifrovacej funkcie	Stredná	**6.5**
17.	Adobe Experience Manager zraniteľnosti	Stredná	**6.1**
18.	Python.org X509 certificate zraniteľnosť	Stredná	**5.9**

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-031

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

Identifikátor

Phoenix Contact FL Switch zraniteľnosti

Popis

Spoločnosť Phoenix Contact vydala bezpečnostnú aktualizáciu na svoje produkty FL Switch, ktorá opravuje viacero bezpečnostných zraniteľností.
Bezpečnostné zraniteľnosti umožňujú vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup do systému a následne v ňom vykonávať zmeny.

Dátum prvého zverejnenia varovania

24.01.2019

CVE

CVE-2017-3735, CVE-2018-13990, CVE-2018-13991, CVE-2018-13992, CVE-2018-13993, CVE-2018-13994

Zasiahnuté systémy

Phoenix Contact FL Switch verzie staršie ako 1.35

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://ics-cert.us-cert.gov/advisories/ICSA-19-024-02

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

Identifikátor

Microsoft Exchange NTLM zraniteľnosť

Popis

Bezpečnostní výskumníci informovali o zraniteľnosti e-mailových serverov Microsoft Exchange. Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov v komponente Exchange Web Services (EWS) PushSubscriptionRequest a umožňuje vzdialenému, autentifikovanému útočníkovi a tiež neautentifikovanému útočníkovi, nachádzajúcemu sa v rovnakom sieťovom segmente, získať neoprávnený prístup do systému.

Dátum prvého zverejnenia varovania

21.01.2019

CVE

-

Zasiahnuté systémy

Microsoft Exchange 2013
Microsoft Exchange 2016
Microsoft Exchange 2019

Následky

Neoprávnený prístup do systému
Eskalácia privilégií

Odporúčania

Spoločnosť Microsoft doposiaľ nevydala aktualizácie riešiace danú zraniteľnosť. Administrátorom odporúčame:
- vypnúť EWS push/pull prihlasovanie príkazmi
New-ThrottlingPolicy -Name NoEWSSubscription - ThrottlingPolicyScope Organization - EwsMaxSubscriptions 0
Restart-WebAppPool -Name MSExchangeServicesAppPool
- odobrať vysoké privilégiá, ktoré Exchange má voči doménovým objektom nástrojom https://github.com/gdedrouas/Exchange-AD-Privesc/blob/master/DomainObject/Fix-DomainObjectDACL.ps1
- povoliť podpisovanie SMB a LDAP
- aplikovať firewallové pravidlá a blokovať komunikáciu z Exchange servera na pracovné stanice

Zdroje

https://dirkjanm.io/abusing-exchange-one-api-call-away-from-domain-admin/
https://www.kb.cert.org/vuls/id/465632/
https://isc.sans.edu/forums/diary/Relaying+Exchanges+NTLM+authentication+to+domain+admin+and+more/24578/

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

Identifikátor

Foxit PhantomPDF zraniteľnosti

Popis

Spoločnosť Foxit Software vydala bezpečnostnú aktualizáciu na svoj produkt Foxit PhantomPDF, ktorá opravuje viacero bezpečnostných zraniteľností.
Bezpečnostné zraniteľnosti umožňujú vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia upravených pdf súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

15.01.2019

CVE

CVE-2019-6727, CVE-2019-6735, CVE-2019-6734, CVE-2019-6733, CVE-2019-6732, CVE-2019-6731, CVE-2019-6730, CVE-2019-6729, CVE-2019-6728, CVE-2019-6727, CVE-2019-5005

Zasiahnuté systémy

Foxit PhantomPDF verzie staršie ako 8.3.9

Následky

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

Zdroje

https://www.foxitsoftware.com/support/security-bulletins.php

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

Identifikátor

Cisco Firepower Threat Defense zraniteľnosť

Popis

Spoločnosť Cisco vydala bezpečnostnú aktualizáciu na svoj produkt Cisco Firepower Threat Defense, ktorá opravuje bezpečnostnú zraniteľnosť v data acquisition (DAQ) komponente.
Bezpečnostná zraniteľnosť spočíva v nesprávnom alokovaní systémových zdrojov a umožňuje vzdialenému, neautentifikovanému útočníkovi spôsobiť zneprístupnenie služieb.

Dátum prvého zverejnenia varovania

23.01.2019

CVE

CVE-2019-1669

Zasiahnuté systémy

Cisco Firepower Threat Defense Software verzia 6.3.0 bežiaca na zariadeniach Firepower 4100 a Firepower 9300

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov. Ak aktualizácia nie je možná, odporúčame vypnúť hardvérovú SSL akceleráciu, ktorá je v základnom nastavení zapnutá.

Zdroje

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190123-firepowertds-bypass

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

Identifikátor

Dräger Infinity Delta zraniteľnosti

Popis

Spoločnosť Dräger vydala bezpečnostnú aktualizáciu na svoj produkt Infinity Delta, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi získať neoprávnený prístup do operačného systému.

Dátum prvého zverejnenia varovania

22.01.2019

CVE

CVE-2018-19010, CVE-2018-19014, CVE-2018-19012

Zasiahnuté systémy

Dräger Delta/Infinity Explorer verzie staršie ako VF10.1

Následky

Neoprávnený prístup do systému
Neoprávnený prístup k citlivým údajom
Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://ics-cert.us-cert.gov/advisories/ICSMA-19-022-01

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

Identifikátor

Cisco Webex Teams client zraniteľnosť

Popis

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

Dátum prvého zverejnenia varovania

23.01.2019

CVE

CVE-2019-1636

Zasiahnuté systémy

Cisco Webex Teams client verzie staršie ako 3.0.10260

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190123-webex-teams

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

Identifikátor

Cisco Webex Player zraniteľnosti

Popis

Spoločnosť Cisco vydala bezpečnostnú aktualizáciu na svoj produkt Webex Player, ktorá opravuje viacero bezpečnostných zraniteľností.
Bezpečnostné zraniteľnosti sú spôsobené nedostatočným overovaním používateľských vstupov a umožňujú lokálnemu, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených ARF a WRF súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

23.01.2019

CVE

CVE-2019-1637, CVE-2019-1638, CVE-2019-1639, CVE-2019-1640, CVE-2019-1641

Zasiahnuté systémy

Cisco Webex Network Recording Player a Webex Player verzie staršie ako WBS32.15.33; 3.0.10260; WBS33.6.1, WBS 33.7.0; 1.3.40; 2.8MR3 SecurityPatch1 a 3.0MR2 SecurityPatch2

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190123-webex-rce

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

Identifikátor

Artifex Software Ghostscript zraniteľnosť

Popis

Spoločnosť Artifex Software vydala bezpečnostnú aktualizáciu na svoj produkt Ghostscript, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia upravených PostScript súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

28.01.2019

CVE

CVE-2019-6116

Zasiahnuté systémy

Artifex Software Ghostscript

Následky

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

Zdroje

https://tools.cisco.com/security/center/viewAlert.x?alertId=59524

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

Identifikátor

Apache HTTP Server zraniteľnosť

Popis

Vývojári systému Apache HTTP Server vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nedostatočným overovaním používateľských vstupov v komponente mod_ssl a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne upravených požiadaviek spôsobiť zneprístupnenie služieb.

Dátum prvého zverejnenia varovania

22.01.2019

CVE

CVE-2019-0190

Zasiahnuté systémy

Apache HTTP Server verzie staršie ako 2.4.38

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://httpd.apache.org/security/vulnerabilities_24.html
https://tools.cisco.com/security/center/viewAlert.x?alertId=59504

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

Identifikátor

Cisco IoT Field Network Director zraniteľnosť

Popis

Spoločnosť Cisco vydala bezpečnostnú aktualizáciu na svoj produkt Cisco IoT Field Network Director, ktorá opravuje bezpečnostnú zraniteľnosť spočívajúcu v nesprávnej implementácii UDP protokolu. Bezpečnostná zraniteľnosť umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania väčšieho množstva UDP paketov spôsobiť zneprístupnenie služieb.

Dátum prvého zverejnenia varovania

23.01.2019

CVE

CVE-2019-1644

Zasiahnuté systémy

Cisco IoT Field Network Director aka Cisco Connected Grid Network Management System verzie staršie ako 3.0

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190123-iot-fnd-dos

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

Identifikátor

LabKey Server viacero zraniteľností

Popis

Spoločnosť LabKey vydala bezpečnostnú aktualizáciu na svoj produkt LabKey Server Community Edition, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť sú spôsobené nedostatočným overovaním používateľských vstupov a umožňujú vzdialenému útočníkovi prostredníctvom XSS útoku vykonať škodlivý kód.

Dátum prvého zverejnenia varovania

24.01.2019

CVE

CVE-2019-3911, CVE-2019-3912, CVE-2019-3913

Zasiahnuté systémy

LabKey Server verzie staršie ako 18.3.0-61806.763

Následky

Vykonanie škodlivého kódu

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.tenable.com/security/research/tra-2019-03
https://threatpost.com/labkey-vulnerabilities-medical-research/141200/

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

Identifikátor

phpMyAdmin zraniteľnosti

Popis

Vývojári phpMyAdmin vydali aktualizáciu svojho produktu, ktorá rieši viacero chýb a bezpečnostných zraniteľností.
Bezpečnostné zraniteľnosti umožňujú vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

22.01.2019

CVE

CVE-2019-6798, CVE-2019-6799

Zasiahnuté systémy

phpMyAdmin verzie staršie ako 4.8.5

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.phpmyadmin.net/security/PMASA-2019-1/
https://www.phpmyadmin.net/security/PMASA-2019-2/
https://gbhackers.com/phpmyadmin-4-8-5-released/amp/

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

Identifikátor

Johnson Controls Facility Explorer zraniteľnosti

Popis

Spoločnosť Johnson Controls vydala bezpečnostnú aktualizáciu na svoj produkt Facility Explorer, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi získať neoprávnený prístup do systému.

Dátum prvého zverejnenia varovania

22.01.2019

CVE

CVE-2017-16744, CVE-2017-16748

Zasiahnuté systémy

Facility Explorer verzie staršie ako 14.6, 14.4u1 a 6.6

Následky

Neoprávnený prístup do systému
Neoprávnená zmena v systéme

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://ics-cert.us-cert.gov/advisories/ICSA-19-022-01

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

Identifikátor

Jenkins cookies zraniteľnosti

Popis

Vývojári nástroja Jenkins vydali aktualizáciu svojho produktu, ktorá rieši viacero bezpečnostných zraniteľností.
Bezpečnostné zraniteľnosti umožňujú vzdialenému, autentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených cookie súborov získať neoprávnený prístup do systému.

Dátum prvého zverejnenia varovania

16.01.2019

CVE

CVE-2019-1003003, CVE-2019-1003004

Zasiahnuté systémy

Jenkins verzie staršie ako 2.160
Jenkins LTS verzie staršie ako 2.150.2

Následky

Neoprávnený prístup do systému

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://jenkins.io/security/advisory/2019-01-16/#SECURITY-901
https://tools.cisco.com/security/center/viewAlert.x?alertId=59508
https://tools.cisco.com/security/center/viewAlert.x?alertId=59509

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

Identifikátor

Cisco Identity Services Engine zraniteľnosť

Popis

Spoločnosť Cisco vydala bezpečnostnú aktualizáciu na svoj produkt Cisco Identity Services Engine, ktorá opravuje bezpečnostnú zraniteľnosť v administrátorskom webovom rozhraní.
Bezpečnostná zraniteľnosť umožňuje vzdialenému, autentifikovanému útočníkovi prostredníctvom zasielania špeciálne upravených HTTP požiadaviek eskalovať svoje privilégiá na napadnutom systéme.

Dátum prvého zverejnenia varovania

23.01.2019

CVE

CVE-2018-15459

Zasiahnuté systémy

Cisco Identity Services Engine

Následky

Eskalácia privilégií

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190123-iot-fnd-dos

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

Identifikátor

7-Zip zraniteľnosť šifrovacej funkcie

Popis

Bezpečnostní výskumníci informovali o zraniteľnosti v komprimačnom nástroji 7-Zip.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov v kryptografickom komponente a umožňuje vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

22.01.2019

CVE

-

Zasiahnuté systémy

7-Zip

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Vývojári 7-Zip doposiaľ nevydala aktualizácie riešiace danú zraniteľnosť. Administrátorom a používateľom odporúčame nepoužívať 7-Zip na šifrovanie súborov.

Zdroje

https://twitter.com/3lbios/status/1087848040583626753?s=19
https://sourceforge.net/p/sevenzip/discussion/45797/thread/6f7607738c/#ce53

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

Identifikátor

Adobe Experience Manager zraniteľnosti

Popis

Spoločnosť Adobe vydala bezpečnostné aktualizácie na svoje produkty Adobe Experience Manager a Adobe Experience Manager Forms, ktoré opravujú viacero bezpečnostných zraniteľností.
Bezpečnostné zraniteľnosti sú spôsobené nedostatočným overovaním používateľských vstupov a umožňujú vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

22.01.2019

CVE

CVE-2018-19724, CVE-2018-19726, CVE-2018-19727

Zasiahnuté systémy

Adobe Experience Manager verzie staršie ako Cumulative Fix Pack for 6.2 SP1 – AEM-6.2-SP1-CFP15; Cumulative Fix Pack for 6.3 SP2 – AEM-6.3.2.2; Service Pack for 6.4 - AEM-6.4.1.0
Adobe Experience Manager Forms verzie staršie ako Cumulative Fix Pack 6.2 SP1-CFP18; Cumulative Fix Pack for 6.3 - AEM-6.3.3.2; Service Pack for 6.4 - AEM-6.4.3.0

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://helpx.adobe.com/security/products/experience-manager/apsb19-09.html
https://helpx.adobe.com/security/products/aem-forms/apsb19-03.html

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 5.9
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Python.org X509 certificate zraniteľnosť

Popis

Vývojári programovacieho jazyka Python vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť v parseri X509 certifikátov.
Bezpečnostná zraniteľnosť umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upraveného X509 certifikátu spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

28.01.0201

CVE

CVE-2019-5010

Zasiahnuté systémy

Python 2.7
Python 3.4
Python 3.5
Python 3.6
Python 3.7

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.talosintelligence.com/vulnerability_reports/TALOS-2019-0758
https://python-security.readthedocs.io/vuln/ssl-crl-dps-dos.html