BEZPEČNOSTNÝ BULLETIN

Týždeň 24. 01. 2018 – 30. 01. 2018

OBSAH BEZPEČNOSTNÉHO BULLETINU

Číslo	Identifikátor	Dôležitosť	CVSS Skóre
1	Siemens Desigo PXC Vulnerability	Kritická	9.8
2	VMware AirWatch, vRealize and vSphere Multiple Vulnerabilties	Vysoká	8.8
3	Lenovo Fingerprint Manager Pro for Windows 7, 8 and 8.1 Insecure Credential Storage	Vysoká	8.8
4	HPE Intelligent Management Center PLAT Multiple Vulnerabilities	Vysoká	8.8
5	Apple macOS/OS X Multiple Flaws	Vysoká	8.8
6	Google Chrome Stable Channel Update for Desktop	Vysoká	8.8
7	Symantec Reporter Vulnerability	Vysoká	8.3
8	FasterXML Code Execution Vulnerability	Vysoká	8.1
9	ClamAV Multiple Vulnerabilities	Vysoká	7.5
10	Philips IntelliSpace Cardiovascular System Vulnerability	Stredná	6.7
11	Fortinet FortiOS XSS Vulnerability	Stredná	5.4
12	Dovecot IMAP/POP3 server DoS vulnerability	Stredná	5.3

Národný bezpečnostný úrad
Budatínska 30
851 06 Bratislava

Mail: *sk-cert@nbu.gov.sk*
Mobil: *+421 903 993 706*
Tel: *+421 2 6869 2858*

SK-CERT
Naša značka:
00099/2018/SKB/OBPr-053

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☐ **Vysoká**	☒ **Kritická**	**CVSS skóre: 9.8**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Siemens Desigo PXC Vulnerability

Popis

Zariadenia Siemens Desigo PXC obsahujú zraniteľnosť, ktorú by vzdialený neautentifikovaný útočník mohol zneužiť na upload škodlivého firmwaru do zariadení.
Zraniteľnosť je spôsobená nedostatočnou implementáciou mechanizmov autentifikácie a útočníkovi umožňuje prevziať celkovú kontrolu nad systémom.

Dátum prvého zverejnenia varovania

24.01.2018 (posledná aktualizácia 25.01.2018)

CVE

CVE-2018-4834

Zasiahnuté systémy

Siemens Desigo Automation Controllers Compact PXC12/22/36-E.D verzie < V6.00.204
Siemens Desigo Automation Controllers Modular PXC00/50/100/200-E.D verzie < V6.00.204
Siemens Desigo Automation Controllers PXC00/64/128-U with Web module verzie < V6.00.204
Siemens Desigo Automation Controllers for Integration PXC001-E.D verzie < V6.00.204
Siemens Desigo Operator Unit PXM20-E verzie < V6.00.204

Následky

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

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu dotknutých zariadení.

Zdroje

https://tools.cisco.com/security/center/viewAlert.x?alertId=56580
https://www.siemens.com/cert/pool/cert/siemens_security_advisory_ssa-824231.pdf
https://ics-cert.us-cert.gov/advisories/ICSA-18-025-02

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

Identifikátor

VMware AirWatch, vRealize and vSphere Multiple Vulnerabilties

Popis

Produkt VMware AirWatch Console obsahuje zraniteľnosť, ktorú by vzdialený neautentifikovaný útočník mohol zneužiť na vykonanie CSRF (Cross-Site Request Forgery) útoku, ktorý by v prípade úspešnosti viedol k stiahnutiu škodlivého softwaru.
Produkty VMware vRealize a vSphere obsahujú zraniteľnosť, ktorú by vzdialený neautentifikovaný útočník mohol zneužiť na vykonanie škodlivého kódu. Zraniteľnosť je spôsobená nesprávnym spracovaním používateľských vstupov.

Dátum prvého zverejnenia varovania

26.01.2018

CVE

CVE-2017-4951

Zasiahnuté systémy

VMware AirWatch Console 9.1.5, 9.2.2
VMware vRealize Automation 7.2, 7.3
VMWare vSphere Integrated Containers 1.3

Následky

Vykonanie škodlivého kódu

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu dotknutých produktov.

Zdroje

https://www.vmware.com/us/security/advisories/VMSA-2018-0006.html
https://tools.cisco.com/security/center/viewAlert.x?alertId=56584

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

Identifikátor

Lenovo Fingerprint Manager Pro for Windows 7, 8 and 8.1 Insecure Credential Storage

Popis

Spoločnosť Lenovo vydala bezpečnostnú aktualizáciu na svoje produkty ThinkPad, ThinkCentre a ThinkStation. Bezpečnostná aktualizácia rieši zraniteľnosť v komponente Fingerprint Manager Pro, ktorá spočíva v nedostatočnom kryptografickom zabezpečení citlivých prihlasovacích údajov, a tiež obsahuje zabudované prihlasovacie heslo umožňujúce lokálnemu útočníkovi eskaláciu privilégií.

Dátum prvého zverejnenia varovania

25.01.2018

CVE

CVE-2017-3762

Zasiahnuté systémy

ThinkPad L560
ThinkPad P40 Yoga, P50s
ThinkPad T440, T440p, T440s, T450, T450s, T460, T540p, T550, T560
ThinkPad W540, W541, W550s
ThinkPad X1 Carbon (Type 20A7, 20A8), X1 Carbon (Type 20BS, 20BT)
ThinkPad X240, X240s, X250, X260
ThinkPad Yoga 14 (20FY), Yoga 460
ThinkCentre M73, M73z, M78, M79, M83, M93, M93p, M93z
ThinkStation E32, P300, P500, P700, P900

Následky

Neoprávnený prístup k citlivým údajom, Eskalácia privilégií

Odporúčania

Administrátorom zasiahnutých systémov odporúčame nainštalovať aktualizáciu uvedeného produktu.

Zdroje

https://support.lenovo.com/sk/en/product_security/len-15999
https://www.theregister.co.uk/2018/01/26/lenovo_thinkpad_fingerprint_manager_vulnerability/

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

Identifikátor

HPE Intelligent Management Center PLAT Multiple Vulnerabilities

Popis

Produkt HPE Intelligent Management Center (iMC) PLAT obsahuje viacero zraniteľností. Najkritickejšie zraniteľnosti by vzdialený neautentifikovaný útočník mohol zneužiť na vykonanie škodlivého kódu.
Ďalšia zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostnej politiky v produkte a vzdialený neautentifikovaný útočník by ju mohol zneužiť na obídenie mechanizmov autentifikácie a získanie prístupu do systému.
Poslednú zraniteľnosť by vzdialený neautentifikovaný útočník mohol zneužiť na získanie prístupu k citlivým údajom.

Dátum prvého zverejnenia varovania

25.01.2018

CVE

CVE-2017-8980, CVE-2017-8981, CVE-2017-8982, CVE-2017-8983, CVE-2017-8984

Zasiahnuté systémy

HP Intelligent Management Center (iMC) 7.3 E0506
HP Intelligent Management Center (iMC) 7.3 E0504P02

Následky

Vykonanie škodlivého kódu, Neoprávnený prístup do systému, Neoprávnený prístup k citlivým údajom

Odporúčania

Spoločnosť HPE vydala bezpečnostnú aktualizáciu, ktorá rieši uvedené zraniteľnosti. Administrátorom odporúčame bezodkladne vykonať aktualizáciu.

Zdroje

https://tools.cisco.com/security/center/viewAlert.x?alertId=56576
https://support.hpe.com/hpsc/doc/public/display?docId=hpesbhf03813en_us
https://support.hpe.com/hpsc/doc/public/display?docId=hpesbhf03810en_us
https://support.hpe.com/hpsc/doc/public/display?docId=hpesbhf03809en_us

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

Identifikátor

Apple macOS/OS X Multiple Flaws

Popis

Spoločnosť Apple vydala bezpečnostné aktualizácie na svoje produkty Apple macOS, iOS, watchOS, tvOS a Safari. Bezpečnostné aktualizácie riešia viacero zraniteľností, najvážnejšie sú okrem známej zraniteľnosti procesorov "Meltdown" tiež zraniteľnosti v komponentoch *IOHIDFamily*, ktoré vzdialenému útočníkovi umožňujú vyvolať chybu v pamäti a vykonať škodlivý kód.

Dátum prvého zverejnenia varovania

23.01.2018

CVE

CVE-2017-5754, CVE-2017-8817, CVE-2018-4082, CVE-2018-4084, CVE-2018-4085, CVE-2018-4086, CVE-2018-4088, CVE-2018-4089, CVE-2018-4090, CVE-2018-4091, CVE-2018-4092, CVE-2018-4093, CVE-2018-4094, CVE-2018-4096, CVE-2018-4097, CVE-2018-4098, CVE-2018-4100

Zasiahnuté systémy

Apple macOS High Sierra, Apple macOS Sierra, Apple macOS X El Capitan, Apple iOS, Apple watchOS, Apple tvOS, Apple Safari

Následky

Vykonanie škodlivého kódu, Eskalácia privilégií, Odopretie služieb

Odporúčania

Administrátorom zasiahnutých systémov odporúčame nainštalovať aktualizácie uvedených produktov.

Zdroje

https://support.apple.com/en-us/HT208465
https://support.apple.com/en-us/HT208463
https://support.apple.com/en-us/HT208475
https://www.securitytracker.com/id/1040267
https://isc.sans.edu/forums/diary/Apple+Updates+Everything+Again/23269/

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

Identifikátor

Google Chrome Stable Channel Update for Desktop

Popis

Spoločnosť Google vydala aktualizáciu na produkt Google Chrome, verzia 64.0.3282.119, ktorá obsahuje opravy 53 bezpečnostných zraniteľností.

Dátum prvého zverejnenia varovania

24.01.2018

CVE

CVE-2018-6031, CVE-2018-6032, CVE-2018-6033, CVE-2018-6034, CVE-2018-6035, CVE-2018-6036, CVE-2018-6037, CVE-2018-6038, CVE-2018-6039, CVE-2018-6040, CVE-2018-6041, CVE-2018-6042, CVE-2018-6043, CVE-2018-6045, CVE-2018-6046, CVE-2018-6047, CVE-2018-6048, CVE-2018-6049, CVE-2018-6050, CVE-2018-6051, CVE-2018-6052, CVE-2018-6053, CVE-2018-6054, CVE-2017-15420

Zasiahnuté systémy

Google Chrome

Následky

Neoprávnený prístup k citlivým údajom, Odopretie služby

Odporúčania

Administrátorom zasiahnutých systémov odporúčame nainštalovať aktualizáciu uvedeného produktu.

Zdroje

https://chromerereleases.googleblog.com/search/label/Stable%20updates

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

Identifikátor

Symantec Reporter Vulnerability

Popis

Produkt Symantec Reporter obsahuje bezpečnostnú zraniteľnosť, ktorú by vzdialený útočník s prístupom k manažmentovému rozhraniu mohol zneužiť na vykonanie brute-force útoku na používateľské účty systému Reporter. Zraniteľnosť je spôsobená chýbajúcimi mechanizmami na limitovanie neúspešných pokusov o prihlásenie. Reporter všetky úspešné a neúspešné pokusy o prihlásenie zaznamenáva.

Dátum prvého zverejnenia varovania

24.01.2018

CVE

CVE-2017-15531

Zasiahnuté systémy

Symantec Reporter 9.5 pred verziou 9.5.4.1
Symantec Reporter 10.1

Následky

Eskalácia privilégií

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu dotknutých produktov a limitovať prístup k manažmentovému rozhraniu systému Reporter.

Zdroje

https://nvd.nist.gov/vuln/detail/CVE-2017-15531
https://www.symantec.com/security-center/network-protection-security-advisories/SA158

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

Identifikátor

FasterXML Code Execution Vulnerability

Popis

Knižnica *jackson-databind* produktu FasterXML obsahuje bezpečnostnú zraniteľnosť, ktorú by vzdialený neautentifikovaný útočník mohol zneužiť na vykonanie škodlivého kódu. Zraniteľnosť je spôsobená nesprávnym overovaním používateľských vstupov metódy *readValue* v rámci objektu *ObjectMapper*.

Dátum prvého zverejnenia varovania

25.01.2018

CVE

CVE-2017-17485

Zasiahnuté systémy

FasterXML jackson-databind 2.7 (.9, .9.1)
FasterXML jackson-databind 2.8 (.0, .1, .2, .3, .4, .5, .6, .7, .8, .8.1, .9, .10)
FasterXML jackson-databind 2.9 (.0, .1, .2, .3)

Následky

Vykonanie škodlivého kódu

Odporúčania

Používateľom odporúčame bezodkladne vykonať aktualizáciu.

Zdroje

https://tools.cisco.com/security/center/viewAlert.x?alertId=56516

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

Identifikátor

ClamAV Multiple Vulnerabilities

Popis

Antivírusový software ClamAV obsahuje viacero bezpečnostných zraniteľností, ktoré by vzdialený neautentifikovaný útočník mohol zneužiť na zneprístupnenie služby alebo vykonanie škodlivého kódu.
Zraniteľnosti spočívajú v nesprávnom overovaní vstupov počas parsovania e-mailov rámci *mbox.c*, spracovávaní PDF dokumentov, *mew* paketov a *tar* archívov a možno ich zneužiť na vyvolanie pretečenia zásobníka.

Dátum prvého zverejnenia varovania

26.01.2018

CVE

CVE-2017-12374, CVE-2017-12375, CVE-2017-12376, CVE-2017-12377, CVE-2017-12378, CVE-2017-12379, CVE-2017-12380

Zasiahnuté systémy

ClamAV pred verziou 0.99.3

Následky

Vykonanie škodlivého kódu, Zneprístupnenie služby

Odporúčania

Používateľom odporúčame bezodkladne vykonať aktualizáciu zraniteľného produktu.

Zdroje

https://tools.cisco.com/security/center/viewAlert.x?alertId=56591
http://blog.clamav.net/2018/01/clamav-0993-has-been-released.html

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre: 6.7**
Klasifikácia	☒ **TLP (WHITE)**	☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**	
Kód sektora (dopad)					

Identifikátor

Philips IntelliSpace Cardiovascular System Vulnerability

Popis

Spoločnosť Philips vydala oznámenie o bezpečnostnej zraniteľnosti vo svojom produkte IntelliSpace Cardiovascular cardiac image and information management systems. Bezpečnostná zraniteľnosť v Electronic Medical Record (EMR) daného softvéru umožňuje vzdialenému útočníkovi využiť nedostatočný spôsob odhlasovania sa z používateľského prostredia, získať autentifikačné údaje používateľov a následne získať prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

24.01.2018

CVE

CVE-2018-5438

Zasiahnuté systémy

Philips IntelliSpace Cardiovascular verzia 2.3.0 a staršie

Následky

Neoprávnený prístup k citlivým údajom, Neoprávnená modifikácia citlivých údajov

Odporúčania

Spoločnosť Philips dosiaľ nevydala aktualizáciu na uvedený produkt. Administrátorom zasiahnutých systémov odporúčame sledovať stránky výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu. Administrátorom zasiahnutých systémov odporúčame zapnúť šifrovanie spojenia v EMR. Taktiež odporúčame používateľom po odhlásení sa z produkčného prostredia vždy zatvoriť webový prehliadač.

Zdroje

https://www.usa.philips.com/healthcare/about/customer-support/product-security
https://ics-cert.us-cert.gov/advisories/ICSMA-18-025-01

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre: 5.4**
Klasifikácia	☒ **TLP (WHITE)**	☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**	
Kód sektora (dopad)					

Identifikátor

Fortinet FortiOS XSS Vulnerability

Popis

Produkt Fortinet FortiOS obsahuje zraniteľnosť, ktorú by vzdialený neautentifikovaný útočník mohol zneužiť na vykonanie XSS (Cross-Site Scripting) útoku.
Zraniteľnosť je spôsobená nedostatočným overovaním HTML kódu v rámci používateľských vstupov. Úspešným XSS útokom by útočník mohol získať prístup k citlivým údajom, ktoré by mohol zneužiť na prípravu nadväzujúcich útokov.

Dátum prvého zverejnenia varovania

29.01.2018

CVE

CVE-2017-14190

Zasiahnuté systémy

FortiOS 5.6.0 až 5.6.2
FortiOS 5.4.0 až 5.4.7
FortiOS 5.2 a nižšie verzie

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Spoločnosť Fortinet vydala bezpečnostnú aktualizáciu riešiacu uvedenú zraniteľnosť. Administrátorom odporúčame bezodkladne vykonať aktualizáciu.

Zdroje

https://fortiguard.com/psirt/FG-IR-17-262
https://tools.cisco.com/security/center/viewAlert.x?alertId=56594

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre: 5.3**
Klasifikácia	☒ **TLP (WHITE)**	☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**	
Kód sektora (dopad)					

Identifikátor

Dovecot IMAP/POP3 server DoS vulnerability

Popis

Produkt Dovecot obsahuje bezpečnostnú zraniteľnosť, ktorú by vzdialený neautentifikovaný útočník mohol zneužiť na zneprístupnenie poskytovaných služieb.
Zraniteľnosť spočíva v nesprávnom mechanizme práce s pamäťou pri prerušení autentifikačného procesu prostredníctvom SASL (Simple Authentication and Security Layer), ktorý útočníkovi umožňuje zahltiť dostupnú pamäť a následne spôsobiť zneprístupnenie služieb produktu.

Dátum prvého zverejnenia varovania

25.01.2018 (posledná aktualizácia 29.01.2018)

CVE

CVE-2017-15132

Zasiahnuté systémy

Dovecot 2.0 až 2.2.33
Dovecot 2.3.0

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu dotknutých produktov.

Zdroje

https://tools.cisco.com/security/center/viewAlert.x?alertId=56595
https://nvd.nist.gov/vuln/detail/CVE-2017-15132
https://access.redhat.com/security/cve/cve-2017-15132