BEZPEČNOSTNÝ BULLETIN

Týždeň 12. 09. 2018 – 18. 09. 2018

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Apple Releases Multiple Security Updates	Vysoká	**8.8**
02.	Multiple Vulnerabilities in PHP Could Allow for Arbitrary Code Execution	Vysoká	**8.8**
03.	SAP Security Patch Day – September 2018	Vysoká	**8.8**
04.	Siemens SCALANCE X300, SCALANCE X408, SCALANCE X414 Denial of Service Vulnerability	Vysoká	**8.6**
05.	Alpine Linux apk-tools Arbitrary Code Execution Vulnerability	Vysoká	**8.1**
06.	Linux Kernel Multiple Vulnerabilities	Vysoká	**7.8**
07.	Fuji Electric V-Server and V-Server Lite Multiple Vulnerabilities	Vysoká	**7.8**
08.	Privilege Escalation Vulnerability in Honeywell Mobile Computers with Android Operating Systems	Vysoká	**7.6**
09.	Wireshark Multiple Denial of Service Vulnerabilities	Vysoká	**7.5**
10.	Siemens TD Keypad Designer Local Privilege Escalation Vulnerability	Vysoká	**7.5**
11.	FreeBSD Information Disclosure and Denial of Service Vulnerability	Vysoká	**7.1**
12.	Apache ActiveMQ, Apache Camel and Apache Mesos Multiple Vulnerabilities	Stredná	**6.5**
13.	Microsoft Windows Server Active Directory Federation Services Server-Side Request Forgery	Stredná	**5.7**
14.	TeamViewer Denial Of Service Vulnerability	Stredná	**4.0**

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:
02049/2018/TS/OKB-142

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

Identifikátor

Apple Releases Multiple Security Updates

Popis

Spoločnosť Apple vydala bezpečnostné aktualizácie na svoje produkty Safari 12, watchOS 5, tvOS 12 a iOS 12, ktoré opravujú viacero bezpečnostných zraniteľností.
Bližšie nešpecifikované bezpečnostné zraniteľnosti spočívajú v nedostatočnej implementácii bezpečnostných mechanizmov a nedostatočným overovaním používateľských vstupov a umožňujú vzdialenému útočníkovi vykonať škodlivý kód na napadnutom systéme a tiež získať prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

17.09.2018

CVE

CVE-2018-4305, CVE-2018-4307, CVE-2018-4313, CVE-2018-4322, CVE-2018-4325, CVE-2018-4329, CVE-2018-4330, CVE-2018-4335, CVE-2018-4338, CVE-2018-4352, CVE-2018-4356, CVE-2018-4362, CVE-2018-4363, CVE-2018-4397, CVE-2018-4195, CVE-2018-5383, CVE-2016-1777,

Zasiahnuté systémy

Apple Support 2.4 for iOS
Safari 12
watchOS 5
tvOS 12
iOS 12

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému, Zneprístupnenie služby, Eskalácia privilégií,
Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://support.apple.com/en-us/HT209106
https://support.apple.com/en-us/HT209107
https://support.apple.com/en-us/HT209108
https://support.apple.com/en-us/HT209109
https://support.apple.com/en-us/HT209117

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

Identifikátor

Multiple Vulnerabilities in PHP Could Allow for Arbitrary Code Execution

Popis

Vývojári skriptovacieho jazyka PHP vydali bezpečnostnú aktualizáciu, ktorá opravuje viacero chýb a bezpečnostných zraniteľností.
Najzávažnejšie bezpečnostné zraniteľnosti by vzdialený neautentifikovaný útočník mohol zneužiť na vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

13.09.2018

CVE

-

Zasiahnuté systémy

PHP 7.2 verzie staršie ako 7.2.10
PHP 7.1 verzie staršie ako 7.1.22
PHP 7.0 verzie staršie ako 7.0.32
PHP 5.6 verzie staršie ako 5.6.38

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-php-could-allow-for-arbitrary-code-execution_2018-101/

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

Identifikátor

SAP Security Patch Day – September 2018

Popis

Spoločnosť SAP vydala bezpečnostné aktualizácie, ktoré opravujú viacero bezpečnostných zraniteľností v portfóliu ich produktov.
Najzávažnejšie sú bezpečnostné zraniteľnosti v produktoch SAP Business One, SAP NetWeaver BI a SAP HANA.
Zraniteľnosť v produkte SAP Business One by vzdialený autentifikovaný útočník mohol zneužiť na neoprávnený prístup k citlivým údajom.
Zraniteľnosť v produkte SAP NetWeaver BI by vzdialený neautentifikovaný útočník prostredníctvom podvrhnutia špeciálne vytvoreného XML súboru mohol zneužiť na realizáciu XXE (XML External Entity) útoku a následné získanie prístupu k citlivým údajom.
Zraniteľnosť v produkte SAP HANA spočíva v nesprávnom overovaní XML súborov v OData parseri a vzdialený neautentifikovaný útočník by ju mohol zneužiť na zneprístupnenie služby databázového servera.

Dátum prvého zverejnenia varovania

11.09.2018

CVE

CVE-2017-12069, CVE-2018-2452, CVE-2018-2454, CVE-2018-2455, CVE-2018-2457, CVE-2018-2458, CVE-2018-2459, CVE-2018-2460, CVE-2018-2461, CVE-2018-2462, CVE-2018-2463, CVE-2018-2464, CVE-2018-2465

Zasiahnuté systémy

SAP Adaptive Server Enterprise verzie 16.0
SAP Business One Android aplikácia verzie 1.2
SAP Business One verzie 9.2, 9.3
SAP Enterprise Financial Services verzie 6.05, 6.06, 6.16, 6.17, 6.18, 8.0
SAP HANA verzie 1.0, 2.0
SAP HCM Fiori "People Profile" (GBX01HR) verzie 6.0
SAP Hybris Commerce verzie 6.*
SAP Mobile Platform verzie 3.0
SAP NetWeaver AS Java verzie 7.10 to 7.11, 7.20, 7.30, 7.31, 7.40, 7.50
SAP NetWeaver BI verzie 7.30, 7.31. 7.40, 7.41, 7.50
SAP Plant Connectivity verzie 15.0
SAP WebDynpro verzie 7.20, 7.30, 7.31, 7.40, 7.50

Následky

Vykonanie škodlivého kódu, Zneprístupnenie služby, Eskalácia privilégií, Neoprávnený prístup k citlivým údajom

Odporúčania
Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje
https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=499356993

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

Identifikátor

Siemens SCALANCE X300, SCALANCE X408, SCALANCE X414 Denial of Service Vulnerability

Popis

Spoločnosť Siemens vydala bezpečnostné aktualizácie, ktoré opravujú bezpečnostnú zraniteľnosť v priemyselných switchoch série SCALANCE X.
Bližšie nešpecifikovaná zraniteľnosť sa nachádza v integrovanom webovom serveri a vzdialený neautentifikovaný útočník by ju prostredníctvom podvrhnutia špeciálne vytvorených paketov mohol zneužiť na vyvolanie reštartu zariadenia a následné zneprístupnenie služby.
Podľa informácií spoločnosti Siemens je zraniteľnosť možné zneužiť prostredníctvom voľne dostupných nástrojov na skenovanie zraniteľností.

Dátum prvého zverejnenia varovania

11.09.2018

CVE

CVE-2018-13807

Zasiahnuté systémy

SCALANCE X300 verzie staršie ako V4.0.0
SCALANCE X408 verzie staršie ako V4.0.0
SCALANCE X414 všetky verzie

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov a zavedením firewallových pravidiel limitovať prístup k integrovanému webovému serveru na porte 443/TCP. Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od Internetu.

Zdroje

https://cert-portal.siemens.com/productcert/pdf/ssa-447396.pdf
https://ics-cert.us-cert.gov/advisories/ICSA-18-254-05

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

Identifikátor

Alpine Linux apk-tools Arbitrary Code Execution Vulnerability

Popis

Vývojári operačného systému Alpine Linux vydali bezpečnostné aktualizácie, ktoré opravujú bezpečnostnú zraniteľnosť v balíku apk-tools.
Bezpečnostná zraniteľnosť spočíva v nesprávnej implementácii spracovania liniek pri extrakcii obsahu APK súborov a vzdialený neautentifikovaný útočník by ju mohol zneužiť na vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému.
Na uvedenú zraniteľnosť je voľne dostupný Proof-of-Concept kód.

Dátum prvého zverejnenia varovania

15.09.2018

CVE

-

Zasiahnuté systémy

Alpine Linux verzie staršie ako 3.8.1

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://alpinelinux.org/posts/Alpine-3.8.1-released.html
https://tools.cisco.com/security/center/viewAlert.x?alertId=58923
https://github.com/alpinelinux/apk-tools/releases

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

Identifikátor

Linux Kernel Multiple Vulnerabilities

Popis

Vývojári linuxového jadra vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje viacero bezpečnostných zraniteľností.
Zraniteľnosti nachádzajúce sa v KVM (Kernel-based Virtual Machine) hypervízore a L2TP (Layer 2 Tunneling Protocol) ovládači by lokálny autentifikovaný útočník prostredníctvom podvrhnutia špeciálne vytvorených vstupov mohol zneužiť na eskaláciu privilégií a úplné narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

12.09.2018

CVE

CVE-2018-9517, CVE-2018-10853

Zasiahnuté systémy

Linux Kernel

Následky

Eskalácia privilégií

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://tools.cisco.com/security/center/viewAlert.x?alertId=58906
https://tools.cisco.com/security/center/viewAlert.x?alertId=58881

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

Identifikátor

Fuji Electric V-Server and V-Server Lite Multiple Vulnerabilities

Popis

Spoločnosť Fuji Electric vydala bezpečnostné aktualizácie, ktoré opravujú viacero bezpečnostných zraniteľností v produktoch V-Server a V-Server Lite.
Najzávažnejšia je zraniteľnosť v produkte V-Server Lite a lokálny neautentifikovaný útočník by ju prostredníctvom podvrhnutia špeciálne vytvorených súborov mohol zneužiť na vyvolanie pretečenia zásobníka a následné vykonanie škodlivého kódu.
Zraniteľnosti v produkte V-Server by vzdialený neautentifikovaný útočník mohol zneužiť na vykonanie škodlivého kódu.

Dátum prvého zverejnenia varovania

11.09.2018 (posledná aktualizácia 13.09.2018)

CVE

CVE-2018-10637, CVE-2018-14809, CVE-2018-14811, CVE-2018-14813, CVE-2018-14815, CVE-2018-14817, CVE-2018-14819, CVE-2018-14823

Zasiahnuté systémy

V-Server verzie 4.0.3.0 a staršie
V-Server Lite verzie 4.0.3.0 a staršie

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 systémom zavedením zoznamu pre riadenie prístupov (ACL). Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od Internetu.

Zdroje

https://ics-cert.us-cert.gov/advisories/ICSA-18-254-01
https://ics-cert.us-cert.gov/advisories/ICSA-18-254-02

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.6**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Privilege Escalation Vulnerability in Honeywell Mobile Computers with Android Operating Systems

Popis

Spoločnosť Honeywell vydala bezpečnostné aktualizácie, ktoré opravujú bezpečnostnú zraniteľnosti v mobilných zariadeniach série CT60, CN80, CT40, CK75, CN75, CT50, D75e, CN51 a EDA s operačným systémom Android.
Bližšie nešpecifikovanú zraniteľnosť by vzdialený neautentifikovaný útočník prostredníctvom podvrhnutia špeciálne vytvorenej Android aplikácie mohol zneužiť na eskaláciu privilégií a neoprávnený prístup k citlivým údajom uloženým v zasiahnutých zariadeniach.

Dátum prvého zverejnenia varovania

13.09.2018

CVE

CVE-2018-14825

Zasiahnuté systémy

EDA51 s operačným systémom Android OS 8.1
CT60, CN80, CT40, EDA50, EDA50k, EDA70, EDA60k s operačným systémom Android OS 7.1
CK75, CN75, CN75e, CT50, D75e, CN51 s operačným systémom Android OS 6.0
CT50, D75e, EDA50k operačným systémom Android 4.4

Následky

Eskalácia privilégií, Vykonanie škodlivého kódu

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov. Rovnako odporúčame poučiť používateľov, aby inštalovali len aplikácie z dôveryhodných zdrojov. Bezpečnostné odporúčania pre zariadenia spoločnosti Honeywell s operačným systémom Android sú dostupné na nasledujúcom odkaze:
https://www.honeywellaidc.com/en/-/media/en/files-public/technical-publications/multi-product/ALLSKU-AND-ENUS-ZY.pdf

Zdroje

https://ics-cert.us-cert.gov/advisories/ICSA-18-256-01

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

Identifikátor

Wireshark Multiple Denial of Service Vulnerabilities

Popis

Vývojári analytického nástroja Wireshark vydali aktualizáciu svojho produktu, ktorá opravuje viacero bezpečnostných zraniteľností.
Uvedené zraniteľnosti by vzdialený neautentifikovaný útočník prostredníctvom podvrhnutia špeciálne vytvorených súborov alebo sieťovej prevádzky mohol zneužiť na zneprístupnenie služieb na zasiahnutom systéme.
Zraniteľnosti sa nachádzajú v komponentoch:
- Bazaar protocol dissector (epan/dissectors/packet-bzr.c)
- zlib decompression dissector (epan/tvbuff_zlib.c)
- IEEE 802.11 protocol dissector (epan/crypt/airpdcap.c)
- InterSwitch Message Protocol (ISMP) dissector (epan/dissectors/packet-ismp.c)
- HTTP2 dissector (epan/dissectors/packet-http2.c)
- Constrained Application Protocol (CoAP) dissector (epan/dissectors/packet-coap.c)
- Multimedia Messaging Service Encapsulation (MMSE) dissector (epan/proto.c)
- Digital Imaging and Communications in Medicine (DICOM) dissector (epan/dissectors/packet-dcm.c)
- Abstract Syntax Notation One (ASN.1) Basic Encoding Rules (BER) dissector (epan/dissectors/packet-ber.c)
- Border Gateway Protocol (BGP) dissector (epan/dissectors/packet-bgp.c)

Na uvedené zraniteľnosti je voľne dostupný Proof-of-Concept kód.

Dátum prvého zverejnenia varovania

13.09.2018 (posledná aktualizácia 15.09.2018)

CVE

CVE-2018-14339, CVE-2018-14340, CVE-2018-14341, CVE-2018-14342, CVE-2018-14343, CVE-2018-14344, CVE-2018-14367, CVE-2018-14368, CVE-2018-14369, CVE-2018-14370

Zasiahnuté systémy

Wireshark verzie 2.6.0 až 2.6.1, 2.4.0 až 2.4.7, 2.2.0 až 2.2.15

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje
https://www.wireshark.org/security/wnpa-sec-2018-34.html
https://www.wireshark.org/security/wnpa-sec-2018-35.html
https://www.wireshark.org/security/wnpa-sec-2018-36.html
https://www.wireshark.org/security/wnpa-sec-2018-37.html
https://www.wireshark.org/security/wnpa-sec-2018-38.html
https://www.wireshark.org/security/wnpa-sec-2018-39.html
https://www.wireshark.org/security/wnpa-sec-2018-40.html
https://www.wireshark.org/security/wnpa-sec-2018-41.html
https://www.wireshark.org/security/wnpa-sec-2018-42.html
https://www.wireshark.org/security/wnpa-sec-2018-43.html

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

Identifikátor

Siemens TD Keypad Designer Local Privilege Escalation Vulnerability

Popis

Spoločnosť Siemens vydala bezpečnostné upozornenie na zraniteľnosť produkte TD Keypad Designer, ktorý slúži na návrh laminátových štítkov pre textové displeje.
Zraniteľnosť spočíva v nesprávnej implementácii nahrávania dynamických knižníc DLL a lokálny autentifikovaný útočník by ju prostredníctvom podvrhnutia špeciálne vytvorených DLL súborov mohol zneužiť na vykonanie škodlivého kódu s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

11.09.2018

CVE

CVE-2018-13806

Zasiahnuté systémy

SIEMENS TD Keypad Designer všetky verzie

Následky

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

Odporúčania

Nakoľko sa jedná o produkty s ukončenou zákazníckou a technickou podporou, spoločnosť Siemens neplánuje vydať bezpečnostné aktualizácie a odporúča vykonať nasledujúce protiopatrenia:
- obmedziť práva na zápis do priečinka s TD projektami len na autorizovaných používateľov
- otvárať len TD projekty pochádzajúce z dôveryhodných zdrojov

Zdroje

https://cert-portal.siemens.com/productcert/pdf/ssa-198330.pdf
https://ics-cert.us-cert.gov/advisories/ICSA-18-254-03

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.1**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

FreeBSD Information Disclusure and Denial of Service Vulnerability

Popis

Vývojári operačného systému FreeBSD vydali bezpečnostnú aktualizáciu, ktorá opravuje bezpečnostnú zraniteľnosť v parseri ELF (Executable and Linkable Format) hlavičiek.
Uvedenú zraniteľnosť by lokálny autentifikovaný útočník prostredníctvom podvrhnutia špeciálne vytvorených ELF súborov mohol zneužiť na vykonanie škodlivého kódu a následné zneprístupnenie služby alebo neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

12.09.2018

CVE

CVE-2018-6924

Zasiahnuté systémy

FreeBSD všetky verzie

Následky

Vykonanie škodlivého kódu, Zneprístupnenie služby, Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.freebsd.org/security/advisories/FreeBSD-SA-18:12.elf.asc
https://securitytracker.com/id?1041646
https://tools.cisco.com/security/center/viewAlert.x?alertId=58907

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

Identifikátor

Apache ActiveMQ, Apache Camel and Apache Mesos Multiple Vulnerabilities

Popis

Spoločnosť Apache vydala bezpečnostné aktualizácie, ktoré opravujú bezpečnostné zraniteľnosti v produktoch Apache ActiveMQ, Apache Camel a Apache Mesos.
Bezpečnostná zraniteľnosť v produkte Apache ActiveMQ spočíva v chýbajúcom overovaní TLS (Transport Layer Security) hostname parametra a vzdialený neautentifikovaný útočník by ju prostredníctvom MITM (Man-In-The-Middle) útoku mohol zneužiť na obídenie bezpečnostných mechanizmov a získanie neoprávneného prístupu do systému.
Zraniteľnosť v produkte Apache Camel spočíva v nedostatočnom overovaní používateľských vstupov v komponente camel-mail a vzdialený neautentifikovaný útočník by ju prostredníctvom podvrhnutia špeciálne vytvorených URL obsahujúcich /../ sekvencie mohol zneužiť na získanie neoprávneného prístupu k citlivým údajom.
Zraniteľnosť v produkte Apache Mesos by vzdialený neautentifikovaný útočník prostredníctvom podvrhnutia špeciálne vytvorených HTTP požiadaviek mohol zneužiť na zneprístupnenie služby.

Dátum prvého zverejnenia varovania

12.09.2018

CVE

CVE-2018-1330, CVE-2018-8041, CVE-2018-11775

Zasiahnuté systémy

Apache ActiveMQ 5.0.0 - 5.15.5
Apache Camel verzie 2.20.0 až 2.20.3, 2.21.0 až 2.21.1 a 2.22.0
Apache Mesos verzie 1.4.0 až 1.5.0

Následky

Neoprávnený prístup do systému. Neoprávnený prístup k citlivým údajom,
Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

http://activemq.apache.org/security-advisories.data/CVE-2018-11775-announcement.txt
https://tools.cisco.com/security/center/viewAlert.x?alertId=58905
https://seclists.org/oss-sec/2018/q3/236

https://exchange.xforce.ibmcloud.com/vulnerabilities/149786
https://seclists.org/oss-sec/2018/q3/240
https://exchange.xforce.ibmcloud.com/vulnerabilities/149831

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 5.7
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Microsoft Windows Server Active Directory Federation Services Server-Side Request Forgery

Popis

Bezpečnostní výskumníci zverejnili informáciu o bezpečnostnej zraniteľnosti v Microsoft Windows Server, ktorá sa nachádza v komponente Active Directory Federation Services. Uvedenú zraniteľnosť by vzdialený autentifikovaný útočník mohol zneužiť na realizáciu SSRF (Server-Side Request Forgery) útokov a vykonanie neoprávnených zmien v systéme.
Na uvedenú zraniteľnosť je voľne dostupný Proof-of-Concept kód.

Dátum prvého zverejnenia varovania

12.09.2018

CVE

CVE-2018-16794

Zasiahnuté systémy

Microsoft Active Directory Federation Services 4.0 pre Microsoft Windows Server

Následky

Neoprávnená zmena v systéme

Odporúčania

Na uvedenú zraniteľnosť v súčasnosti nie sú dostupné aktualizácie. Administrátorom odporúčame sledovať stránky výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu zasiahnutých produktov.

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/149785

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre: 4.0**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

TeamViewer Denial Of Service Vulnerability

Popis

Bezpečnostní výskumníci zverejnili informáciu o bezpečnostnej zraniteľnosti v produkte TeamViewer.
Zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a lokálny neautentifikovaný útočník by ju prostredníctvom podvrhnutia dlhého vstupu do poľa Email Address mohol zneužiť na vyvolanie pádu aplikácie a následné zneprístupnenie služby.
Na uvedenú zraniteľnosť je voľne dostupný Proof-of-Concept kód.

Dátum prvého zverejnenia varovania

13.09.2018

CVE

-

Zasiahnuté systémy

TeamViewer verzie 13.0.100.0

Následky

Zneprístupnenie služby

Odporúčania

Na uvedenú zraniteľnosť v súčasnosti nie sú dostupné aktualizácie. Administrátorom a používateľom odporúčame sledovať stránky výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/149862
https://www.exploit-db.com/exploits/45404/