BEZPEČNOSTNÝ BULLETIN

Týždeň 06. 03. 2019 - 12. 03. 2019

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Hewlett Packard Enterprise Intelligent Management Center zraniteľnosti	Vysoká	**8.8**
02.	RubyGems viacero zraniteľností	Vysoká	**8.8**
03.	Zraniteľnosti Cisco produktov	Vysoká	**8.8**
04.	StackStorm zraniteľnosť	Vysoká	**8.8**
05.	Zraniteľnosť elektronických zabezpečovacích systémov Chuango	Vysoká	**8.8**
06.	IBM WebSphere MQ zraniteľnosti	Vysoká	**8.8**
07.	McAfee Endpoint Security zraniteľnosť	Vysoká	**8.6**
08.	IBM DB2 zraniteľnosti	Vysoká	**8.4**
09.	Apache Qpid Broker-J zraniteľnosť	Vysoká	**7.5**
10.	Apache Mesos zraniteľnosť	Vysoká	**7.5**
11.	Yubico libu2f-host zraniteľnosti	Vysoká	**7.5**
12.	ImageMagick zraniteľnosť	Vysoká	**7.5**
13.	OpenSSL zraniteľnosť	Vysoká	**7.4**
14.	QNAP TS-431 QTS zraniteľnosť	Vysoká	**7.3**

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-073

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

Identifikátor

Hewlett Packard Enterprise Intelligent Management Center zraniteľnosti

Popis

Bezpečnostní výskumníci informovali o zraniteľnostiach v produkte Hewlett Packard Enterprise Intelligent Management Center. Najzávažnejšie bezpečnostné zraniteľnosti sú spôsobené nedostatočným overovaním používateľských vstupov a umožňujú vzdialenému, autentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

04.03.2019

CVE

-

Zasiahnuté systémy

Hewlett Packard Enterprise Intelligent Management Center

Následky

Spoločnosť Hewlett Packard Enterprise doposiaľ nevydala aktualizácie riešiace uvedené zraniteľnosti. Odporúčame aplikovať firewallové pravidlá a sledovať stránky výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu.
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.

Odporúčania

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

Zdroje
https://www.zerodayinitiative.com/advisories/ZDI-19-233/
https://www.zerodayinitiative.com/advisories/ZDI-19-234/
https://www.zerodayinitiative.com/advisories/ZDI-19-235/
https://www.zerodayinitiative.com/advisories/ZDI-19-236/
https://www.zerodayinitiative.com/advisories/ZDI-19-237/
https://www.zerodayinitiative.com/advisories/ZDI-19-238/
https://www.zerodayinitiative.com/advisories/ZDI-19-239/
https://www.zerodayinitiative.com/advisories/ZDI-19-240/
https://www.zerodayinitiative.com/advisories/ZDI-19-241/
https://www.zerodayinitiative.com/advisories/ZDI-19-242/
https://www.zerodayinitiative.com/advisories/ZDI-19-243/
https://www.zerodayinitiative.com/advisories/ZDI-19-244/
https://www.zerodayinitiative.com/advisories/ZDI-19-245/
https://www.zerodayinitiative.com/advisories/ZDI-19-246/
https://www.zerodayinitiative.com/advisories/ZDI-19-247/
https://www.zerodayinitiative.com/advisories/ZDI-19-248/
https://www.zerodayinitiative.com/advisories/ZDI-19-249/
https://www.zerodayinitiative.com/advisories/ZDI-19-250/
https://www.zerodayinitiative.com/advisories/ZDI-19-251/

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

Identifikátor

RubyGems viacero zraniteľností

Popis

Vývojári balíčkovacieho nástroja RubyGems vydali aktualizáciu svojho produktu, ktorá rieši viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť umožňuje útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených súborov vykonať škodlivý kód s následkom úplného narušenia narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

05.03.2019

CVE

CVE-2019-8320, CVE-2019-8321, CVE-2019-8322, CVE-2019-8323, CVE-2019-8324, CVE-2019-8325

Zasiahnuté systémy

RubyGems verzie staršie ako 2.7.9 a 3.0.3

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://blog.rubygems.org/2019/03/05/security-advisories-2019-03.html
https://www.ruby-lang.org/en/news/2019/03/05/multiple-vulnerabilities-in-rubygems/

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

Identifikátor

Zraniteľnosti Cisco produktov

Popis

Spoločnosť Cisco vydala bezpečnostné aktualizácie na svoje produkty NX-OS, FXOS, Enterprise Chat and Email a DNA Center, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť v NX-API module NX-OS je spôsobená nedostatočným overovaním používateľských vstupov a umožňuje vzdialenému, autentifikovanému útočníkovi prostredníctvom zasielania špeciálne upravených paketov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

06.03.2019

CVE

CVE-2019-1585, CVE-2019-1588, CVE-2019-1591, CVE-2019-1593, CVE-2019-1594, CVE-2019-1595, CVE-2019-1596, CVE-2019-1597, CVE-2019-1598, CVE-2019-1599, CVE-2019-1600, CVE-2019-1601, CVE-2019-1602, CVE-2019-1603, CVE-2019-1604, CVE-2019-1605, CVE-2019-1606, CVE-2019-1607, CVE-2019-1608, CVE-2019-1609, CVE-2019-1610, CVE-2019-1611, CVE-2019-1612, CVE-2019-1613, CVE-2019-1614, CVE-2019-1615, CVE-2019-1616, CVE-2019-1617, CVE-2019-1618, CVE-2019-1702, CVE-2019-1707

Zasiahnuté systémy

Cisco NX-OS Software
Cisco FXOS Software
Cisco Enterprise Chat and Email
Cisco DNA Center
MDS 9000 Series Multilayer Switches
Firepower 2100 Series Firewalls
Firepower 4100 Series Next-Generation Firewalls
Firepower 9300 Security Appliance
Nexus 1000V Switch for Microsoft Hyper-V
Nexus 1000V Switch for VMware vSphere
Nexus 2000 Series Fabric Extenders
Nexus 3000 Series Switches
Nexus 3500 Platform Switches
Nexus 5500 Platform Switches
Nexus 5500 Platform Switches
Nexus 5600 Platform Switches
Nexus 6000 Series Switches
Nexus 7000 Series Switches
Nexus 7700 Series Switches
Nexus 9000 Series Switches
Nexus 9500 R-Series Line Cards and Fabric Modules
UCS 6200 Series Fabric Interconnects
UCS 6300 Series Fabric Interconnects
UCS 6400 Series Fabric Interconnects

Následky
Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému Zneprístupnenie služby

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-20190306-aci-controller-privsec https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190306-apic-ipv6 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190306-chatmail-xss https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190306-dna-xss https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190306-nexus-fbr-dos https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190306-nx-os-api-ex https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190306-nx-os-bash-escal https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190306-nxos-privesca https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190306-nxos-netstack https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190306-nxos-fabric-dos https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190306-nxos-cmdinj-1612 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190306-nxos-file-access https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190306-nxos-cmdinj-1609 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190306-nxos-cmdinj-1610 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190306-nxos-cmdinj-1611 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190306-nxos-directory https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190306-nxos-cmdinj-1613 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190306-nx-os-lan-auth https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190306-nxos-escalation https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190306-nxos-npv-dos https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190306-nxos-pe https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190306-nxos-sig-verif https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190306-nxos-privesc https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190306-nxosldap https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190306-aci-shell-escape https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190306-tetra-ace https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190306-nxos-NXAPI-cmdinj https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190306-nxos-cmdinj-1607

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

Identifikátor

StackStorm zraniteľnosť

Popis

Vývojári StackStorm vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť v REST API.
Bezpečnostná zraniteľnosť 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

08.03.2019

CVE

CVE-2019-9580

Zasiahnuté systémy

StackStorm verzie staršie ako 2.10.3 a 2.9.3

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://stackstorm.com/2019/03/08/stackstorm-2-9-3-2-10-3/
https://thehackernews.com/2019/03/stackstorm-security-vulnerability.html

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

Identifikátor

Zraniteľnosť elektronických zabezpečovacích systémov Chuango

Popis

Bezpečnostní výskumníci informovali o zraniteľnosti v elektronických zabezpečovacích systémov výrobcu Chuango. Bezpečnostná zraniteľnosť spočíva v použití statických kódov v 433MHz rádiových diaľkových ovládačoch a umožňuje vzdialenému, neautentifikovanému útočníkovi aktivovať a deaktivovať alarm a tiež vyvolať falošný poplach.

Dátum prvého zverejnenia varovania

11.03.2019

CVE

CVE-2019-9659

Zasiahnuté systémy

Chuango Wifi Alarm System
Chuango Wifi/Cellular Smart Home System H4 Plus
Chuango Wifi Alarm System AWV Plus
Chuango G5W 3G
Chuango GSM/SMS/RFID Touch Alarm System G5 Plus
Chuango GSM/SMS Alarm System G3
Chuango G5W
Chuango Dual-Network Alarm System B11
Chuango PSTN Alarm System A8
Chuango PSTN/LCD/RFID Touch Alarm System A11
Chuango CG-105S On-Site Alarm System
Eminent EM8617 OV2 Wifi Alarm System

Následky

Neoprávnená zmena v systéme

Odporúčania

Spoločnosť Chuango nevydá aktualizácie svojich produktov. Používateľom zasiahnutých zabezpečovacích systémov odporúčame pri ich obsluhe nepoužívať diaľkové ovládania a aplikovať elektromagnetické zatienenie rádiového prijímača riadiacej jednotky.

Zdroje

https://github.com/RiieCco/write-ups/tree/master/CVE-2019-9659

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

Identifikátor

IBM WebSphere MQ zraniteľnosti

Popis

Spoločnosť IBM vydala bezpečnostné aktualizácie na svoj produkt IBM WebSphere MQ, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť umožňuje lokálnemu, autentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

08.03.2019

CVE

CVE-2018-1974, CVE-2018-1998

Zasiahnuté systémy

IBM WebSphere MQ V8
IBM WebSphere MQ V9 LTS
IBM WebSphere MQ V9.1 LTS

Následky

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

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-01.ibm.com/support/docview.wss?uid=ibm10870488
https://www-01.ibm.com/support/docview.wss?uid=ibm10792043

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

Identifikátor

McAfee Endpoint Security zraniteľnosť

Popis

Spoločnosť McAfee vydala bezpečnostnú aktualizáciu na svoj produkt Endpoint Security (ENS), ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených súborov vykonať eskalovať svoje privilégiá.

Dátum prvého zverejnenia varovania

28.02.2019

CVE

CVE-2019-3582

Zasiahnuté systémy

McAfee Endpoint Security ENS 10.6.1 a staršie

Následky

Eskalácia privilégií
Neoprávnená zmena v systéme

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://kc.mcafee.com/corporate/index?page=content&id=SB10254
https://exchange.xforce.ibmcloud.com/vulnerabilities/157964

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

Identifikátor

IBM DB2 zraniteľnosti

Popis

Spoločnosť IBM vydala bezpečnostné aktualizácie na svoj produkt DB2, ktoré opravujú viacero bezpečnostných zraniteľností.
Bližšie nešpecifikované bezpečnostné zraniteľnosti umožňujú lokálnemu, neautentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

07.03.2019

CVE

CVE-2018-1922, CVE-2018-1923, CVE-2018-1978, CVE-2018-1980, CVE-2019-4015, CVE-2019-4016

Zasiahnuté systémy

IBM DB2 verzie V9.7, V10.1, V10.5 a V11.1

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-01.ibm.com/support/docview.wss?uid=ibm10740413
https://exchange.xforce.ibmcloud.com/vulnerabilities/152858
https://exchange.xforce.ibmcloud.com/vulnerabilities/152859
https://exchange.xforce.ibmcloud.com/vulnerabilities/154069
https://exchange.xforce.ibmcloud.com/vulnerabilities/154078
https://exchange.xforce.ibmcloud.com/vulnerabilities/155894

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

Identifikátor

Apache Qpid Broker-J zraniteľnosť

Popis

Vývojári Apache Qpid Broker-J vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov zasiahnutým systémom a umožňuje vzdialenému útočníkovi prostredníctvom zasielania špeciálne upravených AMQP príkazov spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

01.03.2019

CVE

CVE-2019-0200

Zasiahnuté systémy

Qpid Broker-J verzie staršie ako 7.0.7 a 7.1.1

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://issues.apache.org/jira/browse/QPID-8273
https://seclists.org/oss-sec/2019/q1/152
https://tools.cisco.com/security/center/viewAlert.x?alertId=59729

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

Identifikátor

Apache Mesos zraniteľnosť

Popis

Vývojári nástroja Apache Mesos vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov zasiahnutým systémom a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených JSON súborov spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

04.03.2019

CVE

CVE-2018-11793

Zasiahnuté systémy

Apache Mesos verzie staršie ako 1.4.3, 1.5.2, 1.6.2, 1.7.1 a 1.8.0

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://tools.cisco.com/security/center/viewAlert.x?alertId=59725
https://seclists.org/oss-sec/2019/q1/156/
https://lists.apache.org/thread.html/9be975c53e5ad612c7e0af39f5b88837fbfbc32108e587d3d8499844@%3Cdev.mesos.apache.org%3E

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

Identifikátor

Yubico libu2f-host zraniteľnosti

Popis

Spoločnosť Yubico vydala bezpečnostnú aktualizáciu na svoj produkt libu2f-host, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne upravených súborov spôsobiť zneprístupnenie služieb.

Dátum prvého zverejnenia varovania

22.02.2019

CVE

CVE-2018-20340, CVE-2019-9578

Zasiahnuté systémy

Yubico libu2f-host verzie staršie ako 1.1.8

Následky

Zneprístupnenie služby
Vykonanie škodlivého kódu

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/viewAlert.x?alertId=59731
https://tools.cisco.com/security/center/viewAlert.x?alertId=59732

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

Identifikátor

ImageMagick zraniteľnosť

Popis

Vývojári nástroja ImageMagick vydali bezpečnostnú aktualizáciu opravujúcu bezpečnostnú zraniteľnosť. Bezpečnostná zraniteľnosť je spôsobená nekorektnými operáciami s pamäťou a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne upravených súborov spôsobiť zneprístupnenie služieb.

Dátum prvého zverejnenia varovania

17.01.2019

CVE

CVE-2019-7175

Zasiahnuté systémy

ImageMagick verzie staršie ako 7.0.8-25

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://tools.cisco.com/security/center/viewAlert.x?alertId=59746
https://github.com/ImageMagick/ImageMagick/issues/1450

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

Identifikátor

OpenSSL zraniteľnosť

Popis

Vývojári OpenSSL vydali bezpečnostnú aktualizáciu opravujúcu bezpečnostnú zraniteľnosť. Bezpečnostná zraniteľnosť je spôsobená nekorektnou implementáciou šifry ChaCha20-Poly1305 a umožňuje vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup k citlivým údajom a tiež ich modifikovať.

Dátum prvého zverejnenia varovania

06.03.2019

CVE

CVE-2019-1543

Zasiahnuté systémy

Aplikácie využívajúce OpenSSL verzie 1.1.1 a 1.1.0

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://tools.cisco.com/security/center/viewAlert.x?alertId=59743

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

Identifikátor

QNAP TS-431 QTS zraniteľnosť

Popis

Spoločnosť QNAP vydala bezpečnostnú aktualizáciu na svoj produkt QNAP TS-431 QTS, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nedostatočným overovaním používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup do systému.

Dátum prvého zverejnenia varovania

07.03.2019

CVE

-

Zasiahnuté systémy

QNAP TS-431 QTS verzie staršie ako 4.2.2

Následky

Neoprávnený prístup do systému

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/157891
https://www.exploit-db.com/exploits/46506