BEZPEČNOSTNÝ BULLETIN

Týždeň 05. 09. 2018 – 11. 09. 2018

OBSAH BEZPEČNOSTNÉHO BULLETINU

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-136

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

Identifikátor

Google Chrome Stable Channel Update

Popis

Spoločnosť Google vydala bezpečnostnú aktualizáciu, ktorá opravuje viacero chýb a bezpečnostných zraniteľností v internetovom prehliadači Chrome.
Najzávažnejšie bezpečnostné zraniteľnosti by vzdialený neautentifikovaný útočník mohol prostredníctvom podvrhnutia škodlivého webového obsahu zneužiť na vykonanie škodlivého kódu v kontexte webového prehliadača a úplné narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

04.09.2018

CVE

CVE-2018-16065, CVE-2018-16066, CVE-2018-16067, CVE-2018-16068, CVE-2018-16069, CVE-2018-16070, CVE-2018-16071, CVE-2018-16072, CVE-2018-16073, CVE-2018-16074, CVE-2018-16075, CVE-2018-16076, CVE-2018-16077, CVE-2018-16078, CVE-2018-16079, CVE-2018-16080, CVE-2018-16081, CVE-2018-16082, CVE-2018-16083, CVE-2018-16084, CVE-2018-16085, CVE-2018-16086, CVE-2018-16087, CVE-2018-16088

Zasiahnuté systémy

Google Chrome verzie staršie ako 69.0.3497.81

Následky

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

Odporúčania

Administrátorom a používateľom 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://chromereleases.googleblog.com/search/label/Stable%20updates
https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-google-chrome-could-allow-for-arbitrary-code-execution_2018-095/S

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

Identifikátor

Mozilla Firefox Multiple Vulnerabilities

Popis

Spoločnosť Mozilla vydala bezpečnostné aktualizácie, ktoré opravujú viacero zraniteľností v internetových prehliadačoch Firefox a Firefox ESR.
Najzávažnejšie bezpečnostné zraniteľnosti by vzdialený neautentifikovaný útočník mohol prostredníctvom podvrhnutia škodlivého webového obsahu zneužiť na vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

05.09.2018

CVE

CVE-2017-16541, CVE-2018-12375, CVE-2018-12376, CVE-2018-12377, CVE-2018-12378, CVE-2018-12379, CVE-2018-12381, CVE-2018-12382, CVE-2018-12383

Zasiahnuté systémy

Mozilla Firefox verzie staršie ako 62
Mozilla Firefox ESR verzie staršie ako 60.2

Následky

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

Odporúčania

Administrátorom a používateľom 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.mozilla.org/en-US/security/advisories/mfsa2018-21/
https://www.mozilla.org/en-US/security/advisories/mfsa2018-20/
https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-mozilla-firefox-could-allow-for-arbitrary-code-execution_2018-097/

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

Identifikátor

ProtonVPN Privilege Escalation Vulnerability

Popis

Spoločnosť ProtonVPN AG vydala bezpečnostnú aktualizáciu, ktorá opravuje bezpečnostnú zraniteľnosť v produkte ProtonVPN.
Zraniteľnosť sa nachádza vo funkcionalite connect a lokálny autentifikovaný útočník by ju prostredníctvom špeciálne vytvoreného konfiguračného súboru mohol zneužiť na eskaláciu privilégií a vykonanie škodlivého kódu s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.
Na uvedenú zraniteľnosť je dostupný Proof-of-Concept kód.

Dátum prvého zverejnenia varovania

07.09.2018

CVE

CVE-2018-4010

Zasiahnuté systémy

ProtonVPN VPN Client verzie 1.5.1

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.talosintelligence.com/vulnerability_reports/TALOS-2018-0679

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

Identifikátor

NordVPN Privilege Escalation Vulnerability

Popis

Spoločnosť NordVPN vydala bezpečnostnú aktualizáciu, ktorá opravuje bezpečnostnú zraniteľnosť v produkte NordVPN.
Zraniteľnosť sa nachádza vo funkcionalite connect a lokálny autentifikovaný útočník by ju prostredníctvom špeciálne vytvoreného konfiguračného súboru mohol zneužiť na eskaláciu privilégií a vykonanie škodlivého kódu s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.
Na uvedenú zraniteľnosť je dostupný Proof-of-Concept kód.

Dátum prvého zverejnenia varovania

07.09.2018

CVE

CVE-2018-3952

Zasiahnuté systémy

NordVPN verzie 6.14.28.0

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.talosintelligence.com/vulnerability_reports/TALOS-2018-0622

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

Identifikátor

Opsview Monitor Multiple Vulnerabilities

Popis

Spoločnosť Opsview Ltd. vydala bezpečnostné aktualizácie, ktoré opravujú bezpečnostné zraniteľnosti vo webovom manažmentovom rozhraní produktu Opsview Monitor.
Prvá skupina bezpečnostných zraniteľností spočíva v nedostatočnom overovaní používateľských vstupov a vzdialený neautentifikovaný útočník by ju mohol zneužiť na realizáciu XSS (Cross-Site Scripting) útokov alebo na vytvorenie reverzného shell-u. Zraniteľnosti umožňujú zneužitie nasledujúcich parametrov:
/rest - parameter diagnosticsb2ksy
/settings/api/router - parameter data
/rest/config/notificationmethod/testnotification - parameter value
/rest/config/host/test_rancid_connection - parameter rancid_password
Zraniteľnosť CVE-2018-16145 spočíva v nesprávnej konfigurácii privilégií pre skript /etc/init.d/opsview-reporting-module a vzdialený neautentifikovaný útočník by ju mohol zneužiť na vykonanie škodlivého kódu.
Na uvedené zraniteľnosti je dostupný Proof-of-Concept kód.

Dátum prvého zverejnenia varovania

04.09.2018

CVE

CVE-2018-16144, CVE-2018-16145, CVE-2018-16146, CVE-2018-16147, CVE-2018-16148

Zasiahnuté systémy

Opsview Monitor verzie 5.2, 5.3, 5.4

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.coresecurity.com/advisories/opsview-monitor-multiple-vulnerabilities
https://knowledge.opsview.com/v5.4/docs/whats-new
https://knowledge.opsview.com/v5.3/docs/whats-new

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

Identifikátor

Cisco Products Multiple Vulnerabilities

Popis

Spoločnosť Cisco vydala bezpečnostné aktualizácie na mnohé svoje produkty, ktoré opravujú viacero bezpečnostných zraniteľností. Najvážnejšie bezpečnostné zraniteľnosti umožňujú vzdialenému neautentifikovanému útočníkovi získať neoprávnený prístup do systému, vykonať škodlivý kód a spôsobiť úplné narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

05.09.2018

CVE

CVE-2018-0414, CVE-2018-0421, CVE-2018-0422, CVE-2018-0423, CVE-2018-0424, CVE-2018-0425, CVE-2018-0426, CVE-2018-0430, CVE-2018-0431, CVE-2018-0432, CVE-2018-0433, CVE-2018-0434, CVE-2018-0435, CVE-2018-0436, CVE-2018-0438, CVE-2018-0439, CVE-2018-0440, CVE-2018-0444, CVE-2018-0445, CVE-2018-0447, CVE-2018-0450, CVE-2018-0451, CVE-2018-0452, CVE-2018-0454, CVE-2018-0457, CVE-2018-0458, CVE-2018-0459, CVE-2018-0460, CVE-2018-0462, CVE-2018-0463, CVE-2018-11776

Zasiahnuté systémy

Cisco SD-WAN Solution running on the following products: vEdge 100 Series Routers, vEdge 1000 Series Routers, vEdge 2000 Series Routers, vEdge 5000 Series Routers, vManage Network Management System, vEdge Cloud Router Platform, vSmart Controller Software, vBond Orchestrator Software
Cisco Integrated Management Controller running on the following products: Cisco UCS C-Series, Cisco UCS E-Series, 5000 Series Enterprise Network Compute System (ENCS)
Cisco Webex Meetings
Cisco Webex Meetings Suite (WBS31, WBS32, WBS33)
Cisco Webex Meetings Server
Cisco Meeting Server
Cisco Umbrella ERC
Cisco Prime Access Registrar
Cisco Prime Access Registrar Jumpstart
Cisco Prime Collaboration Assurance
Cisco Packaged Contact Center Enterprise
Cisco Data Center Network Manager
Cisco Tetration Analytics
Cisco Network Services Orchestrator

Cisco Enterprise NFV Infrastructure
Cisco Email Security Appliance
Cisco Cloud Services Platform 2100
Cisco Secure Access Control Server

Následky

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

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých systémov, aplikovať firewallové pravidlá a limitovať prístup k zasiahnutým zariadeniam zavedením zoznamu pre riadenie prístupov (ACL).

Zdroje

https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-cisco-products-could-allow-for-remote-code-execution_2018-098/
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180905-rv-routers-overflow
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180905-webex-pe
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180905-webex-id-mod
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180905-umbrella-priv
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180905-umbrella-file-read
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180905-sd-wan-validation
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180905-sd-wan-injection
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180905-sd-wan-escalation
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180905-cpar-dos
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180905-cimc-injection
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180905-cdcnm-escalation
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180905-webex-player-dos
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180905-tetration-xss
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180905-tetration-vulns
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180905-pcce
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180905-pca-xss
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180905-nso-infodis
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180905-nfvis-infodis
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180905-nfvis-dos1
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180905-nfvis-dos
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180905-meeting-csrf
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180905-esa-url-bypass
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180905-dcnm-xss
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180905-csp2100-injection
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180905-acsxxe

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

Identifikátor

Ice Qube Thermal Management Center Multiple Vulnerabilities

Popis

Spoločnosť Ice Qube vydala bezpečnostnú aktualizáciu, ktorá opravuje viacero bezpečnostných zraniteľností v manažmentovom systéme Thermal Management Center. Zraniteľnosti spočívajúce v ukladaní hesiel v podobe otvoreného textu a nedostatočnej implementácii mechanizmov autentifikácie vo webovom rozhraní. Vzdialený neautentifikovaný útočník by ich mohol zneužiť na získanie neoprávneného prístupu k citlivým údajom.

Dátum prvého zverejnenia varovania

06.09.2018

CVE

CVE-2017-14026, CVE-2017-16714

Zasiahnuté systémy

Ice Qube Thermal Management Center verzie staršie ako 4.13

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov. Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od Internetu.

Zdroje

https://ics-cert.us-cert.gov/advisories/ICSA-18-249-01

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

Identifikátor

Opto22 PAC Control Basic and PAC Control Professional Vulnerability

Popis

Spoločnosť Opto22 vydala bezpečnostnú aktualizáciu na svoj programovací softvér PAC Control.
Bezpečnostná zraniteľnosť spočíva v nedostatočným overovaním používateľských vstupov v OptoScript blokoch a lokálny neautentifikovaný útočník by ju mohol zneužiť na vyvolanie pretečenia zásobníka a následné vykonanie škodlivého kódu.

Dátum prvého zverejnenia varovania

28.06.2018

CVE

CVE-2018-04154

Zasiahnuté systémy

PAC Control Basic Versions staršie ako R10.0b
PAC Control Professional Versions staršie ako R10.0b

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov. Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od Internetu.

Zdroje

https://www.opto22.com/support/resources-tools/knowledgebase/kb87547
https://ics-cert.us-cert.gov/advisories/ICSA-18-247-01

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.
Najzávažnejšie zraniteľnosti nachádzajúce sa vo funkciách yurex_read (CVE-2018-16276, drivers/usb/misc/yurex.c) a alarm_timer_sleep (CVE-2018-13053, kernel/time/alarmtimer.c) by lokálny autentifikovaný útočník prostredníctvom podvrhnutia špeciálne vytvorených vstupov mohol zneužiť na eskaláciu privilégií, vykonanie škodlivého kódu alebo zneprístupnenie služby.
Zraniteľnosť CVE-2018-12896 v kernel/time/posix-timers.c spočíva v implementačnej chybe a lokálny autentifikovaný útočník by ju prostredníctvom veľkého množstva systémových volaní rmmap, futex, timer_create a timer_set_time mohol zneužiť na zneprístupnenie služby.
Ostatné zraniteľnosti vo funkciách irda_bind (CVE-2018-6554, net/irda/af_irda.c) a irda_setsockopt (CVE-2018-6555, drivers/staging/irda/net/af_irda.c) by lokálny autentifikovaný útočník mohol zneužiť na zneprístupnenie služby.

Dátum prvého zverejnenia varovania

04.09.2018

CVE

CVE-2018-6554, CVE-2018-6555, CVE-2018-12896, CVE-2018-13053, CVE-2018-16276

Zasiahnuté systémy

Linux kernel verzie staršie ako 4.17.7

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov, ktorá opravuje všetky zraniteľnosti okrem CVE-2018-12896.
Na zraniteľnosť CVE-2018-12896 v súčasnosti nie sú dostupné aktualizácie. Odporúčame sledovať stránky výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu.

Zdroje

https://tools.cisco.com/security/center/viewAlert.x?alertId=58848
https://tools.cisco.com/security/center/viewAlert.x?alertId=58849

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

Identifikátor

cURL and libcurl NTLM Password Overflow Vulnerability

Popis

Vývojári knižnice cURL vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť v implementácii mechanizmov NT LAN Manager (NTLM) autentifikácie.

Bezpečnostná zraniteľnosť vo funkcii Curl_ntlm_core_mk_nt_hash spočíva v implementačnej chybe a nedostatočnom overovaní používateľských vstupov. Vzdialený neautentifikovaný útočník by ju prostredníctvom podvrhnutia používateľského hesla dĺžky presahujúcej 2GB mohol zneužiť na vyvolávanie pretečenia zásobníka a následné vykonanie škodlivého kódu. Uvedenú zraniteľnosť je možné zneužiť iba na 32-bitových systémoch.

Dátum prvého zverejnenia varovania

05.09.2018

CVE

CVE-2018-14618

Zasiahnuté systémy

curl verzie 7.15.4 až 7.61.0

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov a limitovať maximálnu dĺžku hesla.

Zdroje

https://curl.haxx.se/docs/CVE-2018-14618.html
https://access.redhat.com/security/cve/cve-2018-14618
https://tools.cisco.com/security/center/viewAlert.x?alertId=58865

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

Identifikátor

Dell EMC Isilon OneFS and Dell EMC IsilonSD Edge Remote Kernel Crash Vulnerability

Popis

Spoločnosť Dell vydala bezpečnostné aktualizácie, ktoré opravujú bezpečnostnú zraniteľnosť v produktoch Dell EMC Isilon OneFS a Dell EMC IsilonSD Edge.
Bližšie nešpecifikovaná zraniteľnosť sa nachádza v procese isi_drive_d a vzdialený neautentifikovaný útočník by ju prostredníctvom podvrhnutia špeciálne vytvorených dát mohol zneužiť na vyvolanie pádu servera a zneprístupnenie služby.

Dátum prvého zverejnenia varovania

06.09.2018

CVE

CVE-2018-11071

Zasiahnuté systémy

Dell EMC Isilon OneFS verzie 7.1.1.x, 7.2.1.x, 8.0.0.x, 8.0.1.x, 8.1.0.x, 8.1.x až 8.1.1
Dell EMC IsilonSD Edge verzie 8.0.0.x, 8.0.1.x, 8.1.0.x, 8.1.x až 8.1.1

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://seclists.org/fulldisclosure/2018/Sep/9
https://exchange.xforce.ibmcloud.com/vulnerabilities/149568

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

Identifikátor

GoPro Fusion Studio Privilege Escalation Vulnerability

Popis

Bezpečnostní výskumníci informovali o bezpečnostnej zraniteľnosti v produkte GoPro Fusion Studio.
Zraniteľnosť spočíva v implementačnej chybe v službe GoProFusionDeviceDetectionService, pre ktorú je absolútna cesta v parametri BINARY_PATH_NAME definovaná bez úvodzoviek. Lokálny autentifikovaný útočník by zraniteľnosť mohol zneužiť na eskaláciu privilégií a vykonanie škodlivého kódu s oprávneniami úrovne SYSTEM.
Na uvedenú zraniteľnosť je voľne dostupný Proof-of-Concept kód.

Dátum prvého zverejnenia varovania

04.09.2018 (posledná aktualizácia 07.09.2018)

CVE

-

Zasiahnuté systémy

GoPro Fusion Studio verzie 1.2.1.400 (verzia pre Windows)

Následky

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

Odporúčania

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

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/149414
https://www.zeroscience.mk/en/vulnerabilities/ZSL-2018-5487.php
https://packetstormsecurity.com/files/149235

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

Identifikátor

WordPress Thumbnail Processing Multiple Vulnerabilities

Popis

Bezpečnostní výskumníci zverejnili informáciu o zraniteľnostiach v systéme pre správu obsahu Wordpress, ktoré sa nachádzajú v komponente na spracovanie miniatúr obrázkov (Thumbnail Processing).
Zraniteľnosti spočívajú v nedostatočnom overovaní používateľských vstupov a vzdialený autentifikovaný útočník by ich prostredníctvo podvrhnutia špeciálne vytvorených súborov mohol zneužiť na vykonanie škodlivého kódu.

Dátum prvého zverejnenia varovania

07.09.2018

CVE

CVE-2017-1000600, CVE-2018-1000773

Zasiahnuté systémy

WordPress verzie staršie ako 4.8.6

Následky

Vykonanie škodlivého kódu

Odporúčania

Na uvedené zraniteľnosti v súčasnosti nie sú dostupné aktualizácie. Odporúčame uistiť sa, či Vaše webové stránky nie sú založené na systéme pre správu obsahu WordPress v zraniteľnej verzii. V prípade, že áno, odporúčame sledovať stránky výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu redakčného systému na najnovšiu verziu.

Zdroje

https://tools.cisco.com/security/center/viewAlert.x?alertId=58870
https://tools.cisco.com/security/center/viewAlert.x?alertId=58878

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 6.2
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

VMware Content Locker for iOS and AirWatch Agent for iOS Information Disclosure Vulnerabilities

Popis

Spoločnosť VMware vydala bezpečnostné aktualizácie, ktoré opravujú dvojicu bezpečnostných zraniteľností v produktoch Content Locker for iOS a AirWatch Agent for iOS. Najzávažnejšia je bezpečnostná zraniteľnosť v produkte Content Locker for iOS, ktorá spočíva v nedostatočnej implementácii bezpečnostných mechanizmov. Názvy súborov a k nim priradené metadáta nie sú v rámci SQLite databázy softvéru ukladané v šifrovanej podobe. Uvedenú zraniteľnosť by lokálny neautentifikovaný útočník s prístupom k SQLite databáze mohol zneužiť na získanie neoprávneného prístupu k citlivým údajom.
Zraniteľnosť v produkte AirWatch Agent for iOS spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a lokálny neautentifikovaný útočník by ju mohol zneužiť na získanie neoprávneného prístupu k citlivým údajom.

Dátum prvého zverejnenia varovania

05.09.2018

CVE

CVE-2018-6975, CVE-2018-6976

Zasiahnuté systémy

VMware AirWatch Agent for iOS verzie 5.8.1
VMware Content Locker for iOS verzie 4.14

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.vmware.com/security/advisories/VMSA-2018-0023.html
https://exchange.xforce.ibmcloud.com/vulnerabilities/149456
https://exchange.xforce.ibmcloud.com/vulnerabilities/149455