OBSAH BEZPEČNOSTNÉHO BULLETINU

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

Identifikátor

Mozilla Thunderbird Multiple Vulnerabilities

Popis

Spoločnosť Mozilla vydala bezpečnostnú aktualizáciu na produkt Mozilla Thunderbird, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšiu bezpečnostnú zraniteľnosť by vzdialený neautentifikovaný útočník mohol prostredníctvom podvrhnutia špeciálne vytvoreného webového obsahu zneužiť na vykonanie škodlivého kódu.
Aktualizácia tiež opravuje nedávno odhalenú skupinu zraniteľností súhrnne označovaných pojmom EFAIL, ktoré by vzdialený útočník mohol zneužiť na získanie prístupu k citlivým údajom v e-mailovej komunikácii šifrovanej prostredníctvom PGP a S/MIME.

Dátum prvého zverejnenia varovania

18.05.2018 (posledná aktualizácia 21.05.2018)

CVE

CVE-2018-5150, CVE-2018-5154, CVE-2018-5155, CVE-2018-5159, CVE-2018-5161, CVE-2018-5162, CVE-2018-5168, CVE-2018-5170, CVE-2018-5174, CVE-2018-5178, CVE-2018-5183, CVE-2018-5184, CVE-2018-5185

Zasiahnuté systémy

Mozilla Thunderbird 52.7

Následky

Vykonanie škodlivého kódu a narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Používateľom odporúčame vykonať aktualizáciu produktu Mozilla Thunderbird na verziu 52.8.

Zdroje

https://www.mozilla.org/en-US/security/advisories/mfsa2018-13/
https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-mozilla-thunderbird-could-allow-for-arbitrary-code-execution_2018-058/

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

Identifikátor

Cisco Releases Security Updates

Popis

Spoločnosť Cisco vydala bezpečnostné aktualizácie, ktoré opravujú viacero zraniteľností v ich produktovom portfóliu.

Najzávažnejšia zraniteľnosť v **Cisco Identity Services Engine (ISE)** spočíva v nedostatočnom overovaní EAP-TLS certifikátov a vzdialený neautentifikovaný útočník by ju inicializáciou EAP over TLS autentifikácie prostredníctvom špeciálne upraveného EAP-TLS certifikátu mohol zneužiť na zneprístupnenie služieb aplikačného servera ISE. Ostatné zraniteľnosti v Cisco ISE by vzdialený neautentifikovaný útočník mohol zneužiť na realizáciu XSS (Cross-Site Scripting) útokov voči používateľom webového manažmentového rozhrania.

Zraniteľnosť vo webovom manažmentovom rozhraní **Cisco IoT Field Network Director (IoT-FND)** by vzdialený neautentifikovaný útočník prostredníctvom CSRF (Cross-Site Request Forgery) útoku mohol zneužiť na vykonanie príkazov v kontexte prihláseného používateľa.

Zraniteľnosť v **Cisco Meeting Server** by vzdialený neautentifikovaný útočník prostredníctvom podvrhnutia špeciálne upraveného RTP bitstreamu mohol zneužiť zneprístupnenie audio a video služieb servera.

Najzávažnejšia zraniteľnosť v **Cisco Enterprise NFV Infrastructure Software (NFVIS)** spočíva v nedostatočnom overovaní parametrov príkazov v rámci SCP (Secure Copy Protocol) servera a vzdialený autentifikovaný útočník by ju mohol zneužiť na získanie shell-ového prístupu k operačnému systému Linux daného zariadenia. Ostatné zraniteľnosti v Cisco NFVIS by útočník mohol zneužiť na neoprávnený prístup k citlivým údajom.

Zraniteľnosť vo webovom rozhraní **Cisco Unified Communications Manager** a **Cisco Unified Presence** spočíva v nedostatočnom overovaní používateľských vstupov a vzdialený neautentifikovaný útočník by ju mohol zneužiť na vykonanie XSS (Cross-Site Scripting) útoku a vykonanie škodlivého kódu vo webovom prehliadači používateľa.

Webové rozhranie **Cisco TelePresence Server** obsahuje bezpečnostnú zraniteľnosť, ktorú by vzdialený neautentifikovaný útočník mohol zneužiť na vykonanie XFS (Cross-Frame Scripting) útoku a realizáciu click-jackingu.

Produkty **Cisco IP Phone 7800 Series and 8800 Series** obsahujú bezpečnostnú zraniteľnosť v SDP (SIP Session Description Protocol) parseri, ktorá spočíva v nedostatočnom overovaní SCP parametrov. Uvedenú zraniteľnosť by vzdialený neautentifikovaný útočník mohol prostredníctvom podvrhnutia špeciálnych SIP paketov zneužiť na zneprístupnenie služieb.

Zraniteľnosť v produkte **Cisco SocialMiner** spočíva v nesprávnom spracovávaní nových TCP spojení a vzdialený neautentifikovaný útočník by ju mohol prostredníctvom podvrhnutia špeciálnych TCP paketov zneužiť na zneprístupnenie služieb.

Posledná zraniteľnosť v produkte **Cisco Firepower Threat Defense** spočíva v nesprávnom spracovávaní TCP SSL paketov prijatých mimo očakávaného poradia. Vzdialený neautentifikovaný útočník by túto zraniteľnosť mohol zneužiť na zneprístupnenie služby.

Dátum prvého zverejnenia varovania
16.05.2018

CVE
CVE-2018-0270, CVE-2018-0277, CVE-2018-0279, CVE-2018-0280, CVE-2018-0289, CVE-2018-0290, CVE-2018-0297, CVE-2018-0323, CVE-2018-0324, CVE-2018-0325, CVE-2018-0326, CVE-2018-0327, CVE-2018-0328

Zasiahnuté systémy
Cisco ISE, Cisco ISE Express, Cisco ISE Virtual Appliance Cisco Connected Grid Network Management System, Cisco IoT Field Network Director Cisco Meeting Server Cisco Enterprise NFV Infrastructure Software Cisco Unified Communications Manager, Cisco Unified Presence Cisco TelePresence Server Cisco IP Phone 7800 Series and 8800 Series Cisco SocialMiner Cisco Firepower Threat Defense

Následky
Zneprístupnenie služby, Vykonanie škodlivého kódu, Neoprávnený prístup do systému, Neoprávnený prístup k citlivým údajom

Odporúčania
Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov a zariadení.

Zdroje
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180516-iseeap https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180516-ise-xss https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180516-ident-se-xss https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180516-fnd https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180516-msms https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180516-nfvis-path-traversal https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180516-nfvis https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180516-nfvis-cli-command-injection https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180516-cucm-cup-xss https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180516-ip-phone-dos https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180516-socmin-dos https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180516-firepwr-pb

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

Identifikátor

Signal HTML Tag Injection Vulnerability

Popis

Vývojári komunikačnej platformy Signal vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostné zraniteľnosti spočívajúce v nesprávnej implementácii spracovania HTML tagov.
Bezpečnostné zraniteľnosti umožňujú vzdialenému útočníkovi prostredníctvom podvrhnutia špeciálne upravenej správy vykonať škodlivý kód a získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

14.05.2018 (posledná aktualizácia 16.05.2018)

CVE

CVE-2018-10994, CVE-2018-11101

Zasiahnuté systémy

Signal-desktop Messenger verzie staršie ako v1.9.0

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému; Neoprávnený prístup k citlivým údajom

Odporúčania

Používateľom odporúčame vykonať aktualizáciu zasiahnutých produktov.

Zdroje

https://ivan.barreraoro.com.ar/signal-desktop-html-tag-injection
https://ivan.barreraoro.com.ar/signal-desktop-html-tag-injection-variant-2/
https://www.securityweek.com/signal-flaw-allowed-code-execution-no-user-interaction

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

Identifikátor

IBM Products Multiple Vulnerabilities

Popis

Spoločnosť IBM vydala bezpečnostné aktualizácie na svoje produkty IBM FlashSystem, IBM SAN, IBM Storwiz a IBM Spectrum Virtualize, ktoré opravujú viacero bezpečnostných zraniteľností.
Najvážnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému autentifikovanému útočníkovi získať neoprávnený prístup k citlivým údajom, neoprávnene mazať súbory a spôsobiť zneprístupnenie služieb.

Dátum prvého zverejnenia varovania

11.05.2018 (posledná aktualizácia 14.05.2018)

CVE

CVE-2018-1433, CVE-2018-1434, CVE-2018-1438, CVE-2018-1461, CVE-2018-1462, CVE-2018-1463, CVE-2018-1464, CVE-2018-1465, CVE-2018-1466

Zasiahnuté systémy

IBM FlashSystem™ V840, IBM SAN Volume Controller, IBM Storwize V7000, V5000, V3700 a V3500, IBM Spectrum Virtualize Software, IBM Spectrum Virtualize for Public Cloud, IBM FlashSystem V9000

Následky

Neoprávnený prístup k citlivým údajom, Zneprístupnenie služby, Neoprávnená zmena v systéme

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých produktov.

Zdroje

http://www-01.ibm.com/support/docview.wss?uid=ssg1S1012263
http://www-01.ibm.com/support/docview.wss?uid=ssg1S1012282
http://www-01.ibm.com/support/docview.wss?uid=ssg1S1012283

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

Identifikátor

WhatsApp Messenger for iOS Denial of Service Vulnerability

Popis

Produkt WhatsApp Messenger for iOS obsahuje bezpečnostnú zraniteľnosť, ktorú by vzdialený neautentifikovaný útočník mohol prostredníctvom podvrhnutia špeciálne upravených dát zneužiť na poškodenie pamäte a následné zneprístupnenie služieb.

Dátum prvého zverejnenia varovania

16.05.2018

CVE

-

Zasiahnuté systémy

WhatsApp WhatsApp Messenger for iOS 2.18.31

Následky

Zneprístupnenie služby

Odporúčania

Na uvedené zraniteľnosti v súčasnosti nie sú dostupné aktualizácie. Odporúčame sledovať stránky výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu.

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/143408
https://packetstormsecurity.com/files/147645

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

Identifikátor

Denial-of-Service Vulnerability in SIMATIC S7-400

Popis

Spoločnosť Siemens vydala bezpečnostnú aktualizáciu na svoj produkt SIMATIC S7-400, ktorá opravuje bezpečnostnú zraniteľnosť v PLC module.
Bezpečnostná zraniteľnosť je spôsobená nesprávnym spracovaním používateľských vstupov a umožňuje vzdialenému útočníkovi prostredníctvom podvrhnutia špeciálne upravených paketov spôsobiť zneprístupnenie služieb.

Dátum prvého zverejnenia varovania

15.05.2018

CVE

CVE-2018-4850

Zasiahnuté systémy

SIMATIC S7-400 verzie staršie ako 5.2
SIMATIC S7-400H CPU verzie staršie ako 6.0

Následky

Zneprístupnenie služby

Odporúčania

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

Zdroje

https://cert-portal.siemens.com/productcert/pdf/ssa-914382.pdf

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

Identifikátor

Red Hat DHCP Client Script Code Execution Vulnerability

Popis

Spoločnosť Red Hat vydala bezpečnostnú aktualizáciu na svoj produkt Red Hat Enterprise Linux, ktorá opravuje bezpečnostnú zraniteľnosť v NetworkManager skripte v DHCP klientovi.
Bezpečnostná zraniteľnosť umožňuje vzdialenému útočníkovi vydávajúcemu sa za DHCP server, alebo útočníkovi v lokálnej sieti prostredníctvom podvrhnutia špeciálne upravených DHCP odpovedí spôsobiť vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

15.05.2018

CVE

CVE-2018-1111

Zasiahnuté systémy

Red Hat Enterprise Linux Advanced Update Support 6.4, 6.5, 6.6, 7.2
Red Hat Enterprise Linux Extended Update Support 6.7, 7.3, 7.4
Red Hat Enterprise Linux 6, 7
Red Hat Enterprise Linux Server TUS 6.6, 7.2
Red Hat Virtualization 4 Management Agent for RHEL 7 Hosts

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých produtov. Následne odporúčame preveriť integritu databázy a prístupové logy na prítomnosť pokusov o SQL injekciu.

Zdroje

https://access.redhat.com/security/cve/cve-2018-1111
https://access.redhat.com/security/vulnerabilities/3442151
https://www.theregister.co.uk/2018/05/16/red_hat_dhcp_client_bug/
https://thehackernews.com/2018/05/linux-dhcp-hacking.html

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

Identifikátor

GE PACSystems Vulnerabilities

Popis

Spoločnosť GE vydala bezpečnostné aktualizácie na svoje produkty PACSystems RX3i a RXi, ktoré opravujú bližšie nešpecifikovanú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a vzdialený útočník by ju prostredníctvom podvrhnutia špeciálne upravených paketov mohol zneužiť na zneprístupnenie služby.

Dátum prvého zverejnenia varovania

17.05.2018

CVE

CVE-2018-8867

Zasiahnuté systémy

PACSystems RX3i CPE305/310 version 9.20 a staršie,
RX3i CPE330 version 9.21 a staršie,
RX3i CPE 400 version 9.30 a staršie,
PACSystems RSTi-EP CPE 100 všetky verzie
PACSystems CPU320/CRU320 a RXi všetky verzie

Následky

Zneprístupnenie služby

Odporúčania

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

Zdroje

https://ics-cert.us-cert.gov/advisories/ICSA-18-137-01

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

Identifikátor

Nagios XI Multiple Vulnerabilities

Popis

Sieťový monitorovací softvér Nagios XI obsahuje viacero bezpečnostných zraniteľností, ktoré by vzdialený neautentifikovaný útočník mohol zneužiť na vykonanie SQL injekcie a následné zobrazenie, pridávanie alebo úpravu údajov v databáze.

Zraniteľnosti sú spôsobené nedostatočným overovaním používateľských vstupov v:

admin/logbook.php
admin/commandline.php
admin/info.php
admin/menuaccess.php

Pre uvedené zraniteľnosti je voľne dostupný exploit a možno predpokladať ich zneužitie útočníkmi.

Dátum prvého zverejnenia varovania

03.05.2018 (posledná aktualizácia 16.05.2018)

CVE

CVE-2018-10735, CVE-2018-10736, CVE-2018-10737, CVE-2018-10738

Zasiahnuté systémy

Nagios XI verzie 5.2.0 až 5.2.9, 5.4.0 až 5.4.12

Následky

Neoprávnený prístup k citlivým údajom, Neoprávnená zmena v systéme

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov. Následne odporúčame preveriť integritu databázy a prístupové logy na prítomnosť pokusov o SQL injekciu.

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/143489
https://exchange.xforce.ibmcloud.com/vulnerabilities/143490
https://exchange.xforce.ibmcloud.com/vulnerabilities/143491
https://exchange.xforce.ibmcloud.com/vulnerabilities/143492

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

Identifikátor

cURL Multiple Vulnerabilities

Popis

Vývojári produktu cURL vydali bezpečnostnú aktualizáciu, ktorá opravuje viacero bezpečnostných zraniteľností.
Prvá zraniteľnosť spočíva v nesprávnom vyhodnocovaní dlhých odpovedí servera pri ukončovaní FTP spojenia a vzdialený neautentifikovaný útočník by ju prostredníctvom podvrhnutia špeciálne vytvorenej FTP odpovede mohol zneužiť na zneprístupnenie služby a potenciálne vykonanie škodlivého kódu.
Druhú zraniteľnosť by vzdialený neautentifikovaný útočník mohol prostredníctvom podvrhnutia špeciálnych RTSP odpovedí zneužiť na zneprístupnenie služieb a neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

16.05.2018

CVE

CVE-2018-1000300, CVE-2018-1000301

Zasiahnuté systémy

cURL verzie 7.20.0 až 7.59.0

Následky

Zneprístupnenie služby, Potenciálne vykonanie škodlivého kódu, Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých produktov.

Zdroje

https://curl.haxx.se/docs/adv_2018-82c2.html
https://www.securitytracker.com/id/1040933
https://curl.haxx.se/docs/adv_2018-b138.html
https://www.securitytracker.com/id/1040931

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

Identifikátor

Multiple Vulnerabilities in VMware Products

Popis

Spoločnosť VMware vydala bezpečnostné aktualizácie na svoje produkty NSX SD-WAN Edge, ktoré opravujú viacero bezpečnostných zraniteľností.
Produkt VMware NSX SD-WAN Edge obsahuje bezpečnostnú zraniteľnosť v komponente webového rozhrania, ktorú by vzdialený neautentifikovaný útočník mohol zneužiť na vykonanie škodlivého kódu.
Zraniteľnosti v produktoch VMware Workstation and Fusion by vzdialený autentifikovaný útočník mohol zneužiť na zneprístupnenie služby.
Aktualizácia produktov vCenter Server, ESXi, Workstation a Fusion opravuje nedávno odhalenú skupinu zraniteľností niektorých procesorov INTEL, súhrnne označovaných pojmom SpecterNG, ktoré by lokálny útočník mohol zneužiť na neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

15.05.2018

CVE

CVE-2018-6961, CVE-2018-6962, CVE-2018-6963

Zasiahnuté systémy

VeloCloud VMware NSX SD-WAN Edge verzie 2.x, 3.x
VMware vCenter Server (VC) 5.5, 6.0, 6.5, 6.7
VMware vSphere ESXi (ESXi) 5.5, 6.0, 6.5, 6.7
VMware Workstation Pro/Player (Workstation) 14.x
VMware Fusion Pro/Fusion (Fusion) 10.x

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých produktov.

Zdroje

https://www.vmware.com/security/advisories/VMSA-2018-0011.html
https://www.vmware.com/security/advisories/VMSA-2018-0012.html
https://www.vmware.com/security/advisories/VMSA-2018-0013.html

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

Identifikátor

Delta Industrial Automation TPEditor Vulnerability

Popis

Produkt Delta Industrial Automation TPEditor obsahuje bezpečnostnú zraniteľnosť spočívajúcu v nesprávnom overovaní veľkosti TPE dát pred kopírovaním do pamäte.
Uvedenú zraniteľnosť by vzdialený neautentifikovaný útočník mohol prostredníctvom podvrhnutia špeciálne upravených TPE súborov zneužiť na vykonanie škodlivého kódu v kontexte bežiaceho procesu.

Dátum prvého zverejnenia varovania

16.05.2018

CVE

CVE-2018-8871

Zasiahnuté systémy

Delta Industrial Automation TPEditor 1.89

Následky

Vykonanie škodlivého kódu

Odporúčania

Na uvedenú zraniteľnosť v súčasnosti nie sú dostupné aktualizácie. Administrátorom odporúčame poučiť používateľov, aby neotvárali e-maily a prílohy z neoverených zdrojov. Rovnako odporúčame sledovať stránky výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu.

Zdroje

https://www.zerodayinitiative.com/advisories/ZDI-18-468/
https://exchange.xforce.ibmcloud.com/vulnerabilities/143423
https://ics-cert.us-cert.gov/advisories/ICSA-18-137-04

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

Identifikátor

Adobe Acrobat Reader DC Vulnerabilities

Popis

Spoločnosť Adobe vydala bezpečnostnú aktualizáciu svojho produktu Adobe Acrobat Reader DC, ktoré opravujú viacero bezpečnostných zraniteľností.
Najvážnejšia bezpečnostná zraniteľnosť sa nachádza v komponente *Net.Discovery.queryServices* a umožňuje vzdialenému útočníkovi získať neoprávnený prístup k citlivým údajom a vykonať škodlivý kód.

Dátum prvého zverejnenia varovania

15.05.2018

CVE

CVE-2018-4947, CVE-2018-4996

Zasiahnuté systémy

Adobe Acrobat Reader DC 2018.009.20044

Následky

Vykonanie škodlivého kódu, Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých produktov. Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.

Zdroje

https://www.talosintelligence.com/vulnerability_reports/TALOS-2018-0517
https://www.talosintelligence.com/vulnerability_reports/TALOS-2018-0518