BEZPEČNOSTNÝ BULLETIN

Týždeň 27. 02. 2019 - 05. 03. 2019

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	NVIDIA GPU Display Driver zraniteľnosti	Vysoká	**8.8**
02.	FreeBSD zraniteľnosti	Vysoká	**8.8**
03.	Autodesk AutoCAD Products zraniteľnosti	Vysoká	**8.8**
04.	Google Chrome zraniteľnosť	Vysoká	**8.8**
05.	Google Android zraniteľnosti	Vysoká	**8.8**
06.	PSI GridConnect Telecontrol zraniteľnosť	Vysoká	**8.5**
07.	Dovecot zraniteľnosť	Vysoká	**8.2**
08.	KDE kauth zraniteľnosť	Vysoká	**7.8**
09.	Cisco Webex zraniteľnosť	Vysoká	**7.8**
10.	Pivotal Spring Security OAuth zraniteľnosť	Vysoká	**7.6**
11.	F5 BIG-IP zraniteľnosti	Vysoká	**7.5**
12.	Wireshark viacero zraniteľností	Vysoká	**7.5**
13.	GNU C viacero zraniteľností	Vysoká	**7.5**
14.	Zoho ManageEngine ServiceDesk Plus zraniteľnosť	Stredná	**6.5**

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-061

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

Identifikátor

NVIDIA GPU Display Driver zraniteľnosti

Popis

Spoločnosť NVIDIA vydala bezpečnostné aktualizácie na svoj produkt GPU Display Driver, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšie bezpečnostné zraniteľnosti sú spôsobené nedostatočným overovaním používateľských vstupov a umožňujú lokálnemu, autentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

22.02.2019

CVE

CVE-2019-5665, CVE-2019-5666, CVE-2019-5667, CVE-2019-5668, CVE-2019-5669, CVE-2019-5670, CVE-2019-5671, CVE-2019-5672

Zasiahnuté systémy

NVIDIA GPU Display Driver

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://nvidia.custhelp.com/app/answers/detail/a_id/4772
https://www.bleepingcomputer.com/news/security/nvidia-patches-security-issues-in-gpu-display-driver-for-windows-linux/

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

Identifikátor

FreeBSD zraniteľnosti

Popis

Vývojári operačného systému FreeBSD vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje lokálnemu, autentifikovanému útočníkovi prostredníctvom zasielania špeciálne upravených požiadaviek eskalovať svoje privilégiá.

Dátum prvého zverejnenia varovania

05.02.2019

CVE

CVE-2019-5595

Zasiahnuté systémy

FreeBSD 11.2-STABLE verzie staršie ako r343786
FreeBSD 12.0-STABLE verzie staršie ako r343781
FreeBSD 12.0-RELEASE verzie staršie ako 12.0-RELEASE-p3

Následky

Eskalácia privilégií
Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.freebsd.org/security/advisories/FreeBSD-SA-19:01.syscall.asc
https://www.freebsd.org/security/advisories/FreeBSD-SA-19:02.fd.asc
https://exchange.xforce.ibmcloud.com/vulnerabilities/156628
https://exchange.xforce.ibmcloud.com/vulnerabilities/156624
https://nvd.nist.gov/vuln/detail/CVE-2019-5596

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

Identifikátor

Autodesk AutoCAD Products zraniteľnosti

Popis

Spoločnosť Autodesk vydala bezpečnostné aktualizácie na svoje produkty AutoCAD, Civil 3D a Advance Steel, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšie bezpečnostné zraniteľnosti v parsovacej funkcii DXF súborov umožňujú vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených DXF súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

14.02.2019

CVE

CVE-2019-7358, CVE-2019-7359, CVE-2019-7360, CVE-2019-7361

Zasiahnuté systémy

Autodesk Civil 3D
Autodesk Advance Steel
Autodesk AutoCAD

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov. Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené DXF súbory z neznámych zdrojov.
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.autodesk.com/trust/security-advisories/adsk-sa-2019-0001
https://www.talosintelligence.com/vulnerability_reports/TALOS-2018-0680
https://www.talosintelligence.com/vulnerability_reports/TALOS-2018-0682
https://www.talosintelligence.com/vulnerability_reports/TALOS-2018-0670

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

Identifikátor

Google Chrome zraniteľnosť

Popis

Spoločnosť Google vydala bezpečnostnú aktualizáciu, ktorá opravuje bezpečnostnú zraniteľnosť v internetovom prehliadači Chrome.
Bezpečnostná zraniteľnosť v komponente FileReader 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

01.03.2019

CVE

CVE-2019-5786

Zasiahnuté systémy

Google Chrome verzie staršie ako 72.0.3626.121

Následky

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

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých systémov. Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.
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://chromereleases.googleblog.com/2019/03/stable-channel-update-for-desktop.html
https://www.cisecurity.org/advisory/a-vulnerability-in-google-chrome-could-allow-for-arbitrary-code-execution_2019-026/
https://access.redhat.com/security/cve/cve-2019-5786

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

Identifikátor

Google Android zraniteľnosti

Popis

Spoločnosť Google vydala bezpečnostné aktualizácie na svoj operačný systém Android, ktoré opravujú 40 rôznych bezpečnostných zraniteľností.
Najzávažnejšie bezpečnostné zraniteľnosti by mohol vzdialený, neautentifikovaný útočník prostredníctvom podvrhnutia špeciálne vytvorených súborov zneužiť na vykonanie škodlivého kódu v kontexte privilegovaného procesu s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

04.03.2019

CVE

CVE-2017-8252, CVE-2018-10883, CVE-2018-11817, CVE-2018-11958, CVE-2018-11966, CVE-2018-11970, CVE-2018-11971, CVE-2018-13899, CVE-2018-13917, CVE-2018-13918, CVE-2018-20346, CVE-2018-9561, CVE-2018-9563, CVE-2018-9564, CVE-2019-1985, CVE-2019-1989, CVE-2019-1990, CVE-2019-2003, CVE-2019-2004, CVE-2019-2005, CVE-2019-2006, CVE-2019-2007, CVE-2019-2008, CVE-2019-2009, CVE-2019-2010, CVE-2019-2011, CVE-2019-2012, CVE-2019-2013, CVE-2019-2014, CVE-2019-2015, CVE-2019-2016, CVE-2019-2017, CVE-2019-2018, CVE-2019-2019, CVE-2019-2020, CVE-2019-2021, CVE-2019-2022, CVE-2019-2023, CVE-2019-2024, CVE-2019-2025

Zasiahnuté systémy

Operačný systém Android so Security Patch Levels staršími ako 2019-03-05

Následky

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

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých systémov. Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov, nenavštevovali nedôveryhodné webové stránky a neinštalovali neoverené aplikácie.
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://source.android.com/security/bulletin/2019-03-01
https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-google-android-os-could-allow-for-arbitrary-code-execution_2019-027/

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.5**
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

PSI GridConnect Telecontrol zraniteľnosť

Popis

Spoločnosť PSI GridConnect GmbH vydala bezpečnostnú aktualizáciu na svoje produkty Telecontrol a IEC104, ktorá opravuje bezpečnostnú zraniteľnosť vo webovom rozhraní.
Bezpečnostná zraniteľnosť je spôsobená nedostatočným overovaním používateľských vstupov a umožňuje vzdialenému, autentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

28.02.2019

CVE

CVE-2019-6528

Zasiahnuté systémy

Telecontrol Gateway 3G verzie staršie ako 5.1.20 a 6.0.17
Telecontrol Gateway XS-MU verzie staršie ako 5.1.20 a 6.0.17
Telecontrol Gateway VM verzie staršie ako 5.1.20 a 6.0.17
Smart Telecontrol Unit TCG verzie staršie ako 6.0.17
IEC104 Security Proxy verzie staršie ako 2.2.11

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://ics-cert.us-cert.gov/advisories/ICSA-19-059-01

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 8.2
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Dovecot zraniteľnosť

Popis

Vývojári e-mailového servera Dovecot vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi získať neoprávnený prístup do systému.

Dátum prvého zverejnenia varovania

05.02.2019

CVE

CVE-2019-3814

Zasiahnuté systémy

Dovecot verzie staršie ako 2.2.36.1 a 2.3.4.1

Následky

Neoprávnený prístup do systému

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://dovecot.org/list/dovecot/2019-February/114575.html
https://tools.cisco.com/security/center/viewAlert.x?alertId=59690

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

Identifikátor

KDE kauth zraniteľnosť

Popis

Vývojári linuxového prostredia KDE vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť v kauth komponente.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov zasiahnutým systémom a umožňuje lokálnemu, autentifikovanému útočníkovi prostredníctvom zasielania špeciálne upravenej vstupov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

09.02.2019

CVE

CVE-2019-7443

Zasiahnuté systémy

kauth verzie staršie ako 5.55.0

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://kde.org/info/security/advisory-20190209-1.txt
https://tools.cisco.com/security/center/viewAlert.x?alertId=59691

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

Identifikátor

Cisco Webex zraniteľnosť

Popis

Spoločnosť Cisco vydala bezpečnostné aktualizácie na svoje produkt RV110W, RV130W a RV215W, ktoré opravujú bezpečnostnú zraniteľnosť vo funkcii aktualizácie.
Bezpečnostná zraniteľnosť je spôsobená nedostatočným overovaním používateľských vstupov a umožňuje lokálnemu, autentifikovanému útočníkovi prostredníctvom vyvolania procesu aktualizácie vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

27.02.2019

CVE

CVE-2019-1674

Zasiahnuté systémy

Cisco Webex Meetings Desktop App verzie staršie ako 33.6.6
Cisco Webex Productivity Tools verzie staršie ako 33.0.7

Následky

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

Odporúčania

Administrátorom odporúčame bezodkladne 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-20190227-wmda-cmdinj
https://www.secureauth.com/labs/advisories/cisco-webex-meetings-elevation-privilege-vulnerability-version-2

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

Identifikátor

Pivotal Spring Security OAuth zraniteľnosť

Popis

Spoločnosť Pivotal vydala bezpečnostnú aktualizáciu na svoj produkt Spring Security OAuth, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nedostatočným overovaním používateľských vstupov vo funkcii redirect_uri a umožňuje vzdialenému, autentifikovanému útočníkovi prostredníctvom zasielania špeciálne upravených požiadaviek získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

21.02.2019

CVE

CVE-2019-3778

Zasiahnuté systémy

Spring Security OAuth verzie staršie ako 2.3.5, 2.2.4, 2.1.4 a 2.0.17

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://pivotal.io/security/cve-2019-3778

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

Identifikátor

F5 BIG-IP zraniteľnosti

Popis

Spoločnosť F5 vydala bezpečnostnú aktualizáciu na svoj produkt BIG-IP, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť v komponente Traffic Management Microkernel (TMM) umožňuje vzdialenému, neautentifikovanému útočníkovi spôsobiť zneprístupnenie služieb.

Dátum prvého zverejnenia varovania

26.02.2019

CVE

CVE-2019-6592, CVE-2019-6595

Zasiahnuté systémy

F5 BIG-IP verzie staršie ako 14.1.0, 14.1.0.3, 13.1.1.2, 12.1.4, 11.6.3.3

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://support.f5.com/csp/article/K54167061
https://support.f5.com/csp/article/K10065173
https://support.f5.com/csp/article/K91026261

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

Identifikátor

Wireshark viacero zraniteľností

Popis

Vývojári analyzačného nástroja Wireshark vydali aktualizáciu svojho produktu, ktorá rieši viaceré bezpečnostné zraniteľnosti.
Bezpečnostné zraniteľnosti sú spôsobené nedostatočným overovaním používateľských vstupov a umožňujú vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených paketov spôsobiť zneprístupnenie služieb.

Dátum prvého zverejnenia varovania

27.02.2019

CVE

CVE-2019-9208, CVE-2019-9209, CVE-2019-9214

Zasiahnuté systémy

Wireshark verrzie 2.4.0 až 2.4.12 a 2.6.0 až 2.6.6

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.wireshark.org/security/wnpa-sec-2019-06
https://tools.cisco.com/security/center/viewAlert.x?alertId=59705
https://tools.cisco.com/security/center/viewAlert.x?alertId=59706
https://tools.cisco.com/security/center/viewAlert.x?alertId=59707
https://nvd.nist.gov/vuln/detail/CVE-2019-9208
https://nvd.nist.gov/vuln/detail/CVE-2019-9209
https://nvd.nist.gov/vuln/detail/CVE-2019-9214

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

Identifikátor

GNU C viacero zraniteľností

Popis

Vývojári knižnice GNU C vydali aktualizáciu svojho produktu, ktorá rieši viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť vo funkcii parse_reg_exp umožňuje vzdialenému, neautentifikovanému útočníkovi spôsobiť zneprístupnenie služieb.

Dátum prvého zverejnenia varovania

01.03.2019

CVE

CVE-2019-5155, CVE-2019-9169

Zasiahnuté systémy

glibc verzie staršie ako 2.29

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://tools.cisco.com/security/center/viewAlert.x?alertId=59695
https://tools.cisco.com/security/center/viewAlert.x?alertId=59694
https://sourceware.org/bugzilla/show_bug.cgi?id=18986

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

Identifikátor

Zoho ManageEngine ServiceDesk Plus zraniteľnosť

Popis

Spoločnosť Zoho vydala bezpečnostnú aktualizáciu na svoj produkt ManageEngine ServiceDesk Plus, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nedostatočným overovaním používateľských vstupov a umožňuje vzdialenému, autentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených súborov získať neoprávnený prístup do systému.

Dátum prvého zverejnenia varovania

18.02.2019

CVE

CVE-2019-8394

Zasiahnuté systémy

Zoho ManageEngine ServiceDesk Plus verzie staršie ako 10.0 build 10012

Následky

Neoprávnený prístup do systému

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.manageengine.com/products/service-desk/readme.html
https://nvd.nist.gov/vuln/detail/CVE-2019-8394
https://www.exploit-db.com/exploits/46413