BEZPEČNOSTNÝ BULLETIN

Týždeň 05. 08. 2020 - 11. 08. 2020

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:
01439/2020/SK-CERT-196

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

Identifikátor

Google Android viacero zraniteľností

Popis

Spoločnosť Google vydala bezpečnostné aktualizácie na svoj operačný systém Android, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšie bezpečnostné zraniteľnosti umožňujú vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených súborov vykonať škodlivý kód v kontexte privilegovaného procesu s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

04.08.2020

CVE

CVE-2018-13903, CVE-2018-5886, CVE-2019-10562, CVE-2019-10615, CVE-2019-13998, CVE-2019-13999, CVE-2019-14025, CVE-2019-14052, CVE-2019-14056, CVE-2019-14065, CVE-2019-14089, CVE-2019-14115, CVE-2019-14119, CVE-2019-16746, CVE-2020-0108, CVE-2020-0238, CVE-2020-0239, CVE-2020-0240, CVE-2020-0241, CVE-2020-0242, CVE-2020-0243, CVE-2020-0247, CVE-2020-0248, CVE-2020-0249, CVE-2020-0250, CVE-2020-0251, CVE-2020-0252, CVE-2020-0253, CVE-2020-0254, CVE-2020-0255, CVE-2020-0256, CVE-2020-0257, CVE-2020-0258, CVE-2020-0259, CVE-2020-0260, CVE-2020-11115, CVE-2020-11116, CVE-2020-11118, CVE-2020-11120, CVE-2020-11122, CVE-2020-11128, CVE-2020-12464, CVE-2020-3611, CVE-2020-3619, CVE-2020-3624, CVE-2020-3636, CVE-2020-3640, CVE-2020-3643, CVE-2020-3644, CVE-2020-3666, CVE-2020-3667, CVE-2020-3668, CVE-2020-3669, CVE-2020-3675

Zasiahnuté systémy

Operačný systém Android so Security Patch Levels staršími ako 2020-08-05

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/2020-08-01
https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-google-android-os-could-allow-for-remote-code-execution_2020-104/
https://www.securityweek.com/google-patches-over-50-vulnerabilities-android-august-2020-updates

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

Identifikátor

Teltonika Gateway TRB245 - viacero zraniteľností

Popis

Spoločnosť Teltonika vydala aktualizáciu firmvéru pre svoje zariadenia produkty Teltonika Gateway TRB245, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšie bezpečnostné zraniteľnosti spočívajú v nedostatočnej implementácii bezpečnostných mechanizmov a umožňujú vzdialenému, autentifikovanému útočníkovi, eskalovať svoje privilégiá a vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

03.08.2020

CVE

CVE-2020-5770, CVE-2020-5771, CVE-2020-5772, CVE-2020-5773

Zasiahnuté systémy

Teltonika Gateway TRB245 verzie staršie ako TRB2XX_R_00.02.04.3

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.tenable.com/security/research/tra-2020-48
https://exchange.xforce.ibmcloud.com/vulnerabilities/186227
https://exchange.xforce.ibmcloud.com/vulnerabilities/186228
https://exchange.xforce.ibmcloud.com/vulnerabilities/186229
https://exchange.xforce.ibmcloud.com/vulnerabilities/186230

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

Identifikátor

Foxit Reader a PhantomPDF - viacero zraniteľností

Popis

Spoločnosť Foxit Software vydala bezpečnostnú aktualizáciu na svoje produkty Foxit Reader a PhantomPDF, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšie bezpečnostné zraniteľnosti umožňujú vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia upravených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

31.07.2020

CVE

CVE-2020-11493, CVE-2020-12247, CVE-2020-12248, CVE-2020-15637, CVE-2020-15638

Zasiahnuté systémy

Foxit Reader verzie staršie ako 10.0.1
Foxit PhantomPDF verzie staršie ako 10.0.1

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 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://www.zerodayinitiative.com/advisories/ZDI-20-932/
https://www.zerodayinitiative.com/advisories/ZDI-20-933/
https://www.foxitsoftware.com/support/security-bulletins.html#content-2020

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

Identifikátor

Teamviewer - zraniteľnosť

Popis

Spoločnosť TeamViewer GmbH vydala aktualizáciu na svoj produkt Teamviewer, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených súborov získať prístup k citlivým údajom a následne získať neoprávnenú kontrolu nad systémom.

Dátum prvého zverejnenia varovania

05.08.2020

CVE

Zasiahnuté systémy

Teamviewer verzie staršie ako 8.0.258861, 9.0.258860, 10.0.258873, 11.0.258870, 12.0.258869, 13.2.36220, 14.2.56676, 14.7.48350 a 15.8.3

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://www.cisecurity.org/advisory/a-vulnerability-in-teamviewer-cloud-allow-for-offline-password-cracking_2020-106/
https://jeffs.sh/CVEs/CVE-2020-13699.txt
https://nvd.nist.gov/vuln/detail/CVE-2020-13699
https://community.teamviewer.com/t5/Announcements/Statement-on-CVE-2020-13699/td-p/98448

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

Identifikátor

Netgear routre - viacero zraniteľností

Popis

Spoločnosť Netgear vydala aktualizáciu firmvéru pre svoje produkty R6400, R6700, R7000, R7850, R7900, R8000, RS400, a XR300, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť v komponente acsd je spôsobená nedostatočným overovaním používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi, nachádzajúcemu sa v rovnakom sieťovom segmente vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

04.08.2020

CVE

CVE-2020-15635, CVE-2020-15636

Zasiahnuté systémy

Netgear R6400, R6700, R7000, R7850, R7900, R8000, RS400, a XR300 Firmware verzie staršie ako 1.0.4.98

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.zerodayinitiative.com/advisories/ZDI-20-937/
https://www.zerodayinitiative.com/advisories/ZDI-20-936/
https://kb.netgear.com/000062128/Security-Advisory-for-Pre-Authentication-Stack-Overflow-on-R6700v3-PSV-2020-0224
https://kb.netgear.com/000062127/Security-Advisory-for-Pre-Authentication-Buffer-Overflow-on-R6700v3-PSV-2020-0202
https://exchange.xforce.ibmcloud.com/vulnerabilities/186278
https://exchange.xforce.ibmcloud.com/vulnerabilities/186277

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

Identifikátor

Google Chrome - viacero zraniteľností

Popis

Spoločnosť Google vydala aktualizáciu na svoj internetový prehliadač Google Chrome, ktorá opravuje viacero chýb a bezpečnostných zraniteľností.
Najzávažnejšie bezpečnostné zraniteľnosti umožňujú vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upraveného webového obsahu vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

10.08.2020

CVE

CVE-2020-6542, CVE-2020-6543, CVE-2020-6544, CVE-2020-6545, CVE-2020-6546, CVE-2020-6547, CVE-2020-6548, CVE-2020-6549, CVE-2020-6550, CVE-2020-6551, CVE-2020-6552, CVE-2020-6553, CVE-2020-6554, CVE-2020-6555

Zasiahnuté systémy

Google Chrome verzie staršie ako 84.0.4147.125

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 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/2020/08/stable-channel-update-for-desktop.html

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

Identifikátor

PHP viacero zraniteľností

Popis

Vývojári skriptovacieho jazyka PHP vydali bezpečnostnú aktualizáciu, ktorá opravuje viacero chýb a bezpečnostných zraniteľností.
Najzávažnejšie bezpečnostné zraniteľnosti umožňujú vzdialenému, neautentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

20.02.2020

CVE

CVE-2020-7068

Zasiahnuté systémy

PHP verzie staršie ako 7.4.9
PHP verzie staršie ako 7.3.21
PHP verzie staršie ako 7.2.33

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.php.net/ChangeLog-7.php#PHP_7_4
https://www.php.net/manual-lookup.php?pattern=ChangeLog-7.php%237.2.33&lang=en&scope=404quickref
https://www.php.net/manual-lookup.php?pattern=ChangeLog-7.php%237.3.21&lang=en&scope=404quickref
https://www.php.net/manual-lookup.php?pattern=ChangeLog-7.php%237.4.9&lang=en&scope=404quickref

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

Identifikátor

Qualcomm Snapdragon chips - viacero zraniteľností "Achilles"

Popis

Spoločnosť Qualcomm vydala bezpečnostné aktualizácie na portfólio svojich produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Bližšie nešpecifikované bezpečnostné zraniteľnosti v komponente Digital Signal Processor (DSP) umožňujú vzdialenému, autentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

06.08.2020

CVE

CVE-2020-11201, CVE-2020-11202, CVE-2020-11206, CVE-2020-11207, CVE-2020-11208, CVE-2020-11209

Zasiahnuté systémy

Qualcomm Snapdragon Digital Signal Processor chip

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://blog.checkpoint.com/2020/08/06/achilles-small-chip-big-peril/
https://www.darkreading.com/vulnerabilities---threats/400+-qualcomm-chip-vulnerabilities-threaten-millions-of-android-phones/d/d-id/1338613
https://www.theregister.com/2020/08/07/qualcomm_chips_brimming_with_somewhat/
https://www.securityweek.com/vulnerabilities-qualcomm-chips-expose-billions-devices-attacks

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

Identifikátor

Cisco produkty - viacero zraniteľností

Popis

Spoločnosť Cisco vydala bezpečnostné aktualizácie na portfólio svojich produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšie bezpečnostné zraniteľnosti sú spôsobené nedostatočným overovaním používateľských vstupov a umožňujú vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne upravených IPv6 paketov spôsobiť zneprístupnenie služieb.

Dátum prvého zverejnenia varovania

05.08.2020

CVE

CVE-2020-3324, CVE-2020-3346, CVE-2020-3363, CVE-2020-3411, CVE-2020-3412, CVE-2020-3413, CVE-2020-3433, CVE-2020-3434, CVE-2020-3435, CVE-2020-3447, CVE-2020-3448, CVE-2020-3449, CVE-2020-3463, CVE-2020-3464, CVE-2020-3472, CVE-2020-3500, CVE-2020-3501, CVE-2020-3502, CVE-2020-3525, CVE-2020-3532

Zasiahnuté systémy

Cisco 250 Series Smart Switches, 350 Series Managed Switches, 350X Series Stackable Managed Switches, 550X Series Stackable Managed Switches verzie firmvéru staršie ako 2.5.5.47
Cisco DNA Center verzie staršie ako 1.3.1.4
Cisco StarOS verzie staršie ako 21.15.31, 21.16.4, 21.16.c11, 21.17.4, 21.18.3 a 21.19
Cisco AnyConnect Secure Mobility Client for Windows verzie staršie ako 4.9.00086.
Cisco Webex Meetings verzie staršie ako 40.7.0
Cisco Webex Meetings Desktop App verzie staršie ako 40.4.6 a 40.6
Cisco Webex Meetings Desktop App lockdown versions verzie staršie ako 39.5.24
Cisco Webex Meetings Server verzie staršie ako 3.0 MR3 Security Patch 3 a 4.0 MR3 Security Patch 2
Cisco UCS Director verzie staršie ako 6.7.4.1
Cisco ISE verzie staršie ako 2.7p2
Cisco ESA verzie staršie ako 13.5.1
Cisco SMA verzie staršie ako 13.6.1-201
Cisco Cyber Vision Center Software verzie staršie ako 3.0.4 a 3.1.0
Cisco Unified CM and Cisco Unified CM SME verzie 10.5(2)SU10, 11.5(1)SU8, 12.0(1)SU3, 12.5(1)SU2 a staršie
Cisco Unified CM IM&P Service verzie 10.5(2)SU4a, 11.5(1)SU8, 12.0(1), 12.5(1)SU2 a staršie
Cisco Unity Connection verzie 10.5(2)SU10, 11.5(1)SU8, 12.0(1)SU3, 12.5(1)SU2 a staršie
Cisco IOS XR verzie staršie ako 7.1.3, 7.2.1, a 7.3.1
Small Business 200 Series Smart Switches
Small Business 300 Series Managed Switches
Small Business 500 Series Stackable Managed Switches

Následky

Zneprístupnenie služby
Neoprávnený prístup k citlivým údajom
Neoprávnený prístup do systému

Odporúčania
Administrátorom odporúčame bezodkladne 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/content/CiscoSecurityAdvisory/cisco-sa-sbss-ipv6-dos-3bLk6vA
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dna-info-disc-3bz8BCgR
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asr-dos-zJLJFgBf
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-anyconnect-dll-F26WwJW
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-smtdelete-gJDurOgR
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-mttngs-xss-3VbdxDuF
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-mAkmV4qc
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucs-director-xss-O7T8ORYR
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-client-g3zevBcp
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-pass-disclosure-K8p2Nsgg
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cvc-bypass-K99Cb2ff
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-bgp-ErKEqAer
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-sma-log-YxQ6g2kG
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asr5k-ipv6-dos-ce3zhF8m
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-cuc-imp-xss-XtpzfM5e
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-anyconnect-profile-7u3PERKF
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-anyconnect-dos-feXq4tAV

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

Identifikátor

Bitdefender Endpoint Security for Mac - zraniteľnosť

Popis

Spoločnosť Bitdefender vydala aktualizáciu na svoj produkt Bitdefender Endpoint Security for Mac, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

03.08.2020

CVE

CVE-2020-8108

Zasiahnuté systémy

Bitdefender Endpoint Security for Mac verzie staršie ako 4.12.80

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.bitdefender.com/support/security-advisories/insufficient-client-validation-bitdefender-endpoint-security-mac-va-8759/
https://exchange.xforce.ibmcloud.com/vulnerabilities/186207

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

Identifikátor

Pulse Connect Secure a Policy Secure - viacero zraniteľností

Popis

Spoločnosť Pulse Secure vydala bezpečnostné aktualizácie na svoje produkty Connect Secure a Policy Secure, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

27.07.2020

CVE

CVE-2016-2118, CVE-2018-19519, CVE-2019-11507, CVE-2020-12880, CVE-2020-15408, CVE-2020-8204, CVE-2020-8206, CVE-2020-8216, CVE-2020-8217, CVE-2020-8218, CVE-2020-8219, CVE-2020-8220, CVE-2020-8221, CVE-2020-8222

Zasiahnuté systémy

Pulse Connect Secure (PCS) verzie staršie ako 9.1R8
Pulse Policy Secure (PPS) verzie staršie ako 9.1R8

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://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44516
https://nvd.nist.gov/vuln/detail/CVE-2020-8206

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

Identifikátor

Delta Industrial Automation CNCSoft ScreenEditor - zraniteľnosti

Popis

Spoločnosť Delta Electronics vydala bezpečnostnú aktualizáciu na svoj produkt CNCSoft ScreenEditor, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšie bezpečnostné zraniteľnosti sú spôsobené nedostatočným overovaním používateľských vstupov a umožňujú lokálnemu, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

04.08.2020

CVE

CVE-2020-16199, CVE-2020-16201, CVE-2020-16203

Zasiahnuté systémy

Delta Industrial Automation CNCSoft ScreenEditor verzie staršie ako 1.01.26

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://us-cert.cisa.gov/ics/advisories/icsa-20-217-01

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

Identifikátor

WordPress Newsletter plugin - zraniteľnosti

Popis

Vývojári WordPress zásuvného modulu Newsletter vydali bezpečnostnú aktualizáciu, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia 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

03.08.2020

CVE

-

Zasiahnuté systémy

Newsletter plugin verzie staršie ako 6.8.2

Následky

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

Odporúčania

Odporúčame uistiť sa, či Vaše webové stránky nie sú založené na redakčnom systéme Wordpress so zraniteľnou verziou pluginu. V prípade že áno, zabezpečte aktualizáciu redakčného systému a pluginu.
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.wordfence.com/blog/2020/08/newsletter-plugin-vulnerabilities-affect-over-300000-sites/
https://threatpost.com/newsletter-wordpress-plugin-site-takeover/158025/