BEZPEČNOSTNÝ BULLETIN

Týždeň 26. 08. 2020 - 01. 09. 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-213

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.8**
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, nachádzajúcemu sa v rovnakom sieťovom segmente, vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.
Jedna zo zraniteľností je aktívne zneužívaná útočníkmi.

Dátum prvého zverejnenia varovania

26.08.2020

CVE

CVE-2018-0306, CVE-2018-0307, CVE-2019-1896, CVE-2020-3338, CVE-2020-3394, CVE-2020-3397, CVE-2020-3398, CVE-2020-3415, CVE-2020-3452, CVE-2020-3454, CVE-2020-3504, CVE-2020-3517, CVE-2020-3566, CVE-2020-3569

IOC

RP/0/RSP1/CPU0:Aug 28 03:46:10.375 UTC: raw_ip[399]: %PKT_INFRA-PQMON-6-QUEUE_DROP : Taildrop on XIPC queue 1 owned by igmp (jid=1175)
RP/0/RSP0/CPU0:Aug 28 03:46:10.380 UTC: raw_ip[399]: %PKT_INFRA-PQMON-6-QUEUE_DROP : Taildrop on XIPC queue 1 owned by igmp (jid=1175)
RP/0/RSP0/CPU0:Aug 28 03:49:22.850 UTC: dumper[61]: %OS-DUMPER-7-DUMP_REQUEST : Dump request for process pkg/bin/igmp
RP/0/RSP0/CPU0:Aug 28 03:49:22.851 UTC: dumper[61]: %OS-DUMPER-7-DUMP_ATTRIBUTE : Dump request with attribute 7 for process pkg/bin/igmp
RP/0/RSP0/CPU0:Aug 28 03:49:22.851 UTC: dumper[61]: %OS-DUMPER-4-SIGSEGV : Thread 9 received SIGSEGV - Segmentation Fault
RP/0/RSP0/CPU0:Aug 30 17:21:47.653 UTC: igmp[1169]: %HA-HA_WD_LIB-4-RLIMIT : wd_handle_sigxfsz: Reached 90% of RLIMIT_DATA
RP/0/RSP0/CPU0:Aug 30 17:21:47.653 UTC: igmp[1169]: %ROUTING-IPV4_IGMP-4-OOM_STATE_THROTTLE : Received Critical memory depletion warning, stop creating new igmp state
RP/0/RSP1/CPU0:Aug 30 17:23:50.442 UTC: sysmgr[94]: igmp(1) (jid 1169) (pid 121667828) (fail_count 2) abnormally terminated, restart scheduled

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-213

Zasiahnuté systémy

Cisco IOS XR
Cisco FXOS verzie staršie ako 1.1.4.179, 2.0.1.153, 2.1.1.86, 2.2.1.70
Cisco NX-OS Software verzie staršie ako 7.0(3)I7(8) fix nxos.CSCvt39630-n9k_ALL-1.0.0-7.0.3.I7.8.lib32_n9000.rpm
Cisco UCS 6200, 6300, and 6400 Series Fabric Interconnects verzie staršie ako 3.2(3o), 4.0(4i) a 4.1(1c)
Cisco ASA Software verzie staršie ako 9.6.4.42, 9.8.4.20, 9.9.2.74, 9.10.1.42, 9.12.3.12, 9.13.1.10 a 9.14.1.10
Cisco FTD Software verzie staršie ako 6.2.3.16, 6.4.0.9 + Hot Fix, 6.6.0.1,6.3.0.5 + Hot Fix, 6.3.0.6, 6.4.0.9 + Hot Fix, 6.4.0.10, 6.6.0.1, 6.5.0.4 + Hot Fix, 6.5.0.5 a 6.6.0.1
Cisco UCS C-Series and S-Series Servers verzie staršie ako 2.0(13o), 3.0(4k), 4.0(2f), 4.0(4b)
Cisco IMC Software Release verzie staršie ako 3.2(8)
MDS 9000 Series Multilayer Switches verzie staršie ako 8.1(1a) a 8.2(1)
Nexus 1000V Series Switches verzie staršie ako 5.2(1)SV3(3.15)
Nexus 1100 Series Cloud Services Platforms verzie staršie ako 5.2(1)SV3(3.15)
Nexus 2000 Series Fabric Extenders verzie staršie ako 7.3(3)N1(1)
Nexus 3000 Series Switches verzie staršie ako 7.0(3)I7(4)
Nexus 3500 Platform Switches verzie staršie ako 7.0(3)I7(4)
Nexus 3600 Platform Switches
Nexus 5500 Platform Switches verzie staršie ako 7.3(3)N1(1)
Nexus 5600 Platform Switches verzie staršie ako 7.3(3)N1(1)
Nexus 6000 Series Switches verzie staršie ako 7.3(3)N1(1)
Nexus 7000 Series Switches verzie staršie ako 8.1(2) a 8.2(1)
Nexus 7700 Series Switches verzie staršie ako 8.1(2) a 8.2(1)
Nexus 9000 Series Switches in standalone NX-OS mode verzie staršie ako 7.0(3)I7(4)
Nexus 9500 R-Series Line Cards and Fabric Modules verzie staršie ako 7.0(3)F3(3a)

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému
Eskalácia privilégií
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). Taktiež odporúčame v nastaveniach Cisco IOS XR limitovať objem IGMP dátového toku príkazom "lpts pifib hardware police flow igmp rate ".
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://us-cert.cisa.gov/ncas/current-activity/2020/08/27/cisco-releases-security-updates https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fxos-nxos-cfs-dos-dAmnymbd https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-ro-path-KJuQhB86 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-dvmrp-memexh-dSmpdvfz https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucs-cli-dos-GQUxCnTe https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190821-imc-cmdinject-1896 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-pim-memleak-dos-tC8eP7uw https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180620-nx-os-cli-execution https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180620-nx-os-cli-injection https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-callhome-cmdinj-zkxzSCY https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxosbgp-nlri-dos-458rG2OQ https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxosbgp-mvpn-dos-K8kbCrJp https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-n3n9k-priv-escal-3QhXJBC https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-dme-rce-cbE3nhZS https://www.securityweek.com/attackers-actively-targeting-cisco-ios-xr-vulnerability

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

Identifikátor

Mozilla Firefox a Thunderbird - viacero zraniteľností

Popis

Spoločnosť Mozilla vydala bezpečnostné aktualizácie na svoje produkty Firefox a Thunderbird, ktoré opravujú viacero bezpečnostných zraniteľností.
Bezpečnostné zraniteľnosti umožňujú vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.
Zraniteľnosti sú v súčasnosti aktívne zneužívané útočníkmi.

Dátum prvého zverejnenia varovania

25.08.2020

CVE

CVE-2020-12400, CVE-2020-12401, CVE-2020-15663, CVE-2020-15664, CVE-2020-15665, CVE-2020-15666, CVE-2020-15667, CVE-2020-15668, CVE-2020-15669, CVE-2020-15670, CVE-2020-6829

Zasiahnuté systémy

Firefox verzie staršie ako 80
Firefox ESR verzie staršie ako 68.12 a 78.2
Thunderbird verzie staršie 68.12 a 78.2

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.mozilla.org/en-US/security/advisories/mfsa2020-38/
https://www.mozilla.org/en-US/security/advisories/mfsa2020-36/
https://www.mozilla.org/en-US/security/advisories/mfsa2020-37/
https://www.mozilla.org/en-US/security/advisories/mfsa2020-40/
https://www.mozilla.org/en-US/security/advisories/mfsa2020-41/

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-2020-6558, CVE-2020-6559, CVE-2020-6560, CVE-2020-6561, CVE-2020-6562, CVE-2020-6563, CVE-2020-6564, CVE-2020-6565, CVE-2020-6566, CVE-2020-6567, CVE-2020-6568, CVE-2020-6569, CVE-2020-6570, CVE-2020-6571

Zasiahnuté systémy

Google Chrome verzie staršie ako 85.0.4183.83

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_25.html
https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-google-chrome-could-allow-for-arbitrary-code-execution_2020-121/
https://exchange.xforce.ibmcloud.com/vulnerabilities/187224
https://exchange.xforce.ibmcloud.com/vulnerabilities/187214

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

Identifikátor

Trend Micro Apex One - viacero zraniteľností

Popis

Spoločnosť Trend Micro vydala bezpečnostné aktualizácie na svoj produkt Apex One, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšie bezpečnostné zraniteľnosti umožňujú lokálnemu, autentifikovanému útočníkovi eskalovať svoje privilégiá.

Dátum prvého zverejnenia varovania

28.08.2020

CVE

CVE-2020-24556, CVE-2020-24557, CVE-2020-24558, CVE-2020-24559

Zasiahnuté systémy

Trend Micro Apex One verzie staršie ako Patch 3 b8378, macOS Patch 1 a Aug 2020 Monthly Patch (2008)

Následky

Eskalácia privilégií
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://success.trendmicro.com/solution/000263632
https://exchange.xforce.ibmcloud.com/vulnerabilities/187509
https://exchange.xforce.ibmcloud.com/vulnerabilities/187508
https://exchange.xforce.ibmcloud.com/vulnerabilities/187511
https://www.zerodayinitiative.com/advisories/ZDI-20-1094/
https://www.zerodayinitiative.com/advisories/ZDI-20-1093/
https://www.zerodayinitiative.com/advisories/ZDI-20-1096/

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

Identifikátor

F5 BIG-IP - viacero zraniteľností

Popis

Spoločnosť F5 informovala o bezpečnostných zraniteľnostiach vo svojich produktoch BIG-IP.
Bezpečnostné zraniteľnosti umožňujú vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne upravených súborov spôsobiť zneprístupnenie služby.
Bezpečnostná zraniteľnosť v iControl REST API je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a 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

26.08.2020

CVE

CVE-2020-5902, CVE-2020-5921, CVE-2020-5922, CVE-2020-5926

Zasiahnuté systémy

BIG-IP (LTM, AAM, Advanced WAF, AFM, Analytics, APM, ASM, DDHD, DNS, FPS, GTM, Link Controller, PEM, SSLO) verzie staršie ako 16.0.0, 15.1.0.5, 15.0.1.4, 14.1.2.7, 13.1.3.4, 12.1.5.2

Následky

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

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

Zdroje

https://support.f5.com/csp/article/K42830212
https://support.f5.com/csp/article/K20606443
https://support.f5.com/csp/article/K00103216

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

Identifikátor

Mitsubishi Electric viacero produktov - zraniteľnosť

Popis

Spoločnosť Mitsubishi Electric informovala o bezpečnostnej zraniteľnosti v portfóliu svojich produktov. Bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi vykonávať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

31.08.2020

CVE

CVE-2020-16226

Zasiahnuté systémy
QJ71MES96 všetky verzie QJ71WS96 všetky verzie Q06CCPU-V všetky verzie Q24DHCCPU-V všetky verzie Q24DHCCPU-VG všetky verzie R12CCPU-V všetky verzie RD55UP06-V všetky verzie RD55UP12-V všetky verzie RJ71GN11-T2 všetky verzie RJ71EN71 všetky verzie QJ71E71-100 všetky verzie LJ71E71-100 všetky verzie QJ71MT91 všetky verzie RD78Gn(n=4,8,16,32,64) všetky verzie RD78GHV všetky verzie RD78GHW všetky verzie NZ2GACP620-60 všetky verzie NZ2GACP620-300 všetky verzie NZ2FT-MT všetky verzie NZ2FT-EIP všetky verzie Q03UDECPU sériové číslo 22081 a staršie QnUDEHCPU(n=04/06/10/13/20/26/50/100) sériové číslo 22081 a staršie QnUDVCPU(n=03/04/06/13/26) sériové číslo 22031 a staršie QnUDPVCPU(n=04/06/13/2) sériové číslo 22031 a staršie LnCPU(-P)(n=02/06/26) sériové číslo 22051 a staršie L26CPU-(P)BT sériové číslo 22051 a staršie RnCPU(n=00/01/02) verzie staršie ako 19 RnCPU(n=04/08/16/32/120) verzie staršie ako 51 RnENCPU(n=04/08/16/32/120) verzie staršie ako 51 RnSFCPU (n=08/16/32/120) všetky verzie RnPCPU(n=08/16/32/120) všetky verzie RnPSFCPU(n=08/16/32/120) všetky verzie FX5U(C)-**M*/** Sériové čísla 17X**** alebo novšie: verzie staršie ako 1.211 Sériové čísla 179**** a staršie: verzie staršie ako 1.071 FX5UC-32M*/**-TS verzie staršie ako 1.211 FX5UJ-**M*/** verzie staršie ako 1.001 FX5-ENET všetky verzie FX5-ENET/IP všetky verzie FX3U-ENET-ADP všetky verzie FX3GE-**M*/** všetky verzie FX3U-ENET všetky verzie FX3U-ENET-L všetky verzie FX3U-ENET-P502 všetky verzie FX5-CCLGN-MS všetky verzie IU1-1M20-D všetky verzie LE7-40GU-L všetky verzie GOT2000 Series GT21 Model všetky verzie GS Series všetky verzie GOT1000 Series GT14 Model všetky verzie GT25-J71GN13-T2 všetky verzie FR-A800-E Series všetky verzie FR-F800-E Series všetky verzie FR-A8NCG, vyrobené v auguste 2020 a skôr FR-E800-EPA Series vyrobené v júli 2020 a skôr FR-E800-EPB Series vyrobené v júli 2020 a skôr Conveyor Tracking Application APR-nTR3FH, APR-nTR6FH, APR-nTR12FH, APR-nTR20FH(n=1,2) všetky verzie (produkty so skončenou technickou podporou) MR-JE-C všetky verzie MR-J4-TM všetky verzie

Následky
Neoprávnené zmeny v systéme

Odporúčania
Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov a zabezpečiť komunikáciu medzi systémami prostredníctvom virtuálnej privátnej siete VPN. Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje
https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2020-009_en.pdf https://us-cert.cisa.gov/ics/advisories/icsa-20-245-01