BEZPEČNOSTNÝ BULLETIN

Týždeň 17. 06. 2020 - 23. 06. 2020

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Cisco produkty - viacero zraniteľností	Vysoká	**8.8**
02.	Plex Media Server - viacero zraniteľností	Vysoká	**8.8**
03.	Baxter produkty - viacero zraniteľností	Vysoká	**8.6**
04.	Webroot PC Agent - zraniteľnosti	Vysoká	**8.2**
05.	VideoLAN VLC Media Player - zraniteľnosť	Vysoká	**7.8**
06.	Pulse Secure Desktop Client - zraniteľnosť	Vysoká	**7.8**
07.	Drupal CMS - viacero zraniteľností	Vysoká	**7.5**
08.	Johnson Controls exacqVision - zraniteľnosť	Stredná	**6.8**

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-156

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 v Cisco Webex umožňujú vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

17.06.2020

CVE

CVE-2020-3236, CVE-2020-3241, CVE-2020-3242, CVE-2020-3244, CVE-2020-3245, CVE-2020-3263, CVE-2020-3268, CVE-2020-3269, CVE-2020-3274, CVE-2020-3275, CVE-2020-3276, CVE-2020-3277, CVE-2020-3278, CVE-2020-3279, CVE-2020-3286, CVE-2020-3287, CVE-2020-3288, CVE-2020-3289, CVE-2020-3290, CVE-2020-3291, CVE-2020-3292, CVE-2020-3293, CVE-2020-3294, CVE-2020-3295, CVE-2020-3296, CVE-2020-3336, CVE-2020-3337, CVE-2020-3342, CVE-2020-3347, CVE-2020-3350, CVE-2020-3354, CVE-2020-3355, CVE-2020-3356, CVE-2020-3360, CVE-2020-3361, CVE-2020-3362, CVE-2020-3364, CVE-2020-3368

Zasiahnuté systémy

Cisco Webex Meetings verzie staršie ako WBS 39.5.25, WBS 40.4.10 a WBS 40.6.0
Cisco Webex Meetings Server verzie staršie ako 4.0MR3 Security Patch 1
Cisco RV320 a RV325 Dual Gigabit WAN VPN Routers verzie staršie ako 1.5.1.11.
Cisco RV016, RV042, a RV082 Routers verzie staršie ako 4.2.3.14.
Cisco TelePresence Collaboration Endpoint verzie staršie ako 9.12.3, 9.10.2, 9.9.4 a 9.8.0
Cisco RoomOS Software verzie staršie ako May Drop 2 2020
Cisco Small Business RV110W Wireless-N VPN Firewall verzie staršie ako 1.2.2.8
Cisco Small Business RV130 VPN Router verzie staršie ako 1.0.3.55
Cisco Small Business RV130W Wireless-N Multifunction VPN Router verzie staršie ako 1.0.3.55
Cisco Small Business RV215W Wireless-N VPN Router verzie staršie ako 1.3.1.7
Cisco Enterprise NFVIS verzie staršie ako 4.1.1.
Cisco NSO verzie staršie ako 4.7.7.3 a 5.1.4.2.
Cisco DCNM verzie 11.3(1) a staršie
Cisco ASR 5000 Aggregation Services Routers verzie staršie ako 21.18.0
Cisco UCS Director verzie staršie ako 6.7.4.0.
Cisco IP Phones Series 7800 a Series 8800
Cisco Unified Communications Manager verzia 12.8(1) a staršie
Cisco SSM On-Prem verzie staršie ako 8-202004.
Cisco AMP for Endpoints - Linux verzie staršie ako 1.12.4
Cisco AMP for Endpoints - MacOS verzie staršie ako 1.12.4
ClamAV verzie staršie ako 0.103 a 0.102.4
Cisco AsyncOS for Cisco ESA verzie staršie ako 13.5.0.
Cisco IOS XR

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

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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-token-zPvEjKN
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-routers-injection-tWC7krKQ
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-tp-cmd-inj-7ZpWhvZb
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-client-mac-X7vp65BL
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-client-url-fcmpdfVY
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-routers-stack-vUxHmnNz
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-routers-Rj5JRfF8
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dcnm-stored-xss-eUyGPqxm
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dcnm-stored-xss-VyE4bNAh
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asr5k-ecs-bypass-2LqfPCL
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dcnm-stored-xss-VyE4bNAh
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asr5k-ecs-bypass-2LqfPCL
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-xracl-zbWSWREt
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dcnm-stored-xss-eUyGPqxm
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-on-prem-access-ctrl-fpQRfdpf
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-client-NBmqM9vt
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-umbrella-open-redire-UgK9dWK4
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucsd-task-path-trav-d67ZuAk7
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucsd-info-disclosure-gSMU8EKT
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-phone-logs-2O7f7ExM
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nso-info-disclosure-WdNvBTNq
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nfvis-ptrav-SHMzzwVR
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-famp-ZEpdXy
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-url-bypass-WO4BZ75s
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dcnm-stored-xss-yJyqBJGU

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

Identifikátor

Plex Media Server - viacero zraniteľností

Popis

Spoločnosť Plex vydala bezpečnostnú aktualizáciu na svoj produkt Media Server, ktorá opravuje viacero bezpečnostných zraniteľností.
Bezpečnostné zraniteľnosti sú spôsobené 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

16.06.2020

CVE

CVE-2020-5740, CVE-2020-5741, CVE-2020-5742

Zasiahnuté systémy

Plex Media Server verzie staršie ako 1.18.2

Následky

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

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/blog/tenable-research-discloses-multiple-vulnerabilities-in-plex-media-server
https://www.bleepingcomputer.com/news/security/plex-fixes-media-server-bugs-allowing-full-system-takeover/
https://medium.com/tenable-techblog/examining-a-phishing-vector-in-plex-media-server-2044edf6bd48

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

Identifikátor

Baxter produkty - viacero zraniteľností

Popis

Spoločnosť Baxter informovala o viacerých bezpečnostných zraniteľnostiach, nachádzajúcich sa v ich medicínskych produktoch.
Kritické bezpečnostné zraniteľnosti spočívajú v nedostatočnej implementácii bezpečnostných mechanizmov a existencii používateľských účtov s predvoleným heslom a umožňujú vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup do systému a vykonať neoprávnené zmeny.

Dátum prvého zverejnenia varovania

18.06.2020

CVE

CVE-2020-12035, CVE-2020-12036, CVE-2020-12037, CVE-2020-12039, CVE-2020-12040, CVE-2020-12041, CVE-2020-12043, CVE-2020-12045, CVE-2020-12047, CVE-2020-12048

Zasiahnuté systémy

Baxter Sigma Spectrum v6.x model 35700BAX
Baxter Spectrum v8.x model 35700BAX2
Baxter Sigma Spectrum v6.x with Wireless Battery Modules v9, v11, v13, v14, v15, v16, v20D29, v20D30, v20D31, and v22D24
Baxter Spectrum v8.x with Wireless Battery Modules v17, v20D29, v20D30, v20D31, and v22D24
Baxter Spectrum Wireless Battery Modules v17, v20D29, v20D30, v20D31, and v22D24
Baxter Spectrum LVP v8.x with Wireless Battery Modules v17, v20D29, v20D30, v20D31, and v22D24
Baxter Phoenix Hemodialysis Delivery System SW 3.36 a 3.40
Baxter PrismaFlex verzie staršie ako 8.2x
Baxter PrisMax verzie staršie ako v3
Baxter ExactaMix verzie staršie ako 1.4 (EM1200) a 1.13 (EM2400)

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnený prístup do systému
Neoprávnená zmena v systéme
Zneprístupnenie služby

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.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje
https://www.us-cert.gov/ics/advisories/icsma-20-170-04
https://www.us-cert.gov/ics/advisories/icsma-20-170-03
https://www.us-cert.gov/ics/advisories/icsma-20-170-02
https://www.us-cert.gov/ics/advisories/icsma-20-170-01

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

Identifikátor

Webroot PC Agent - zraniteľnosti

Popis

Spoločnosť Webroot vydala bezpečnostnú aktualizáciu na svoj produkt PC Agent, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne upravených požiadaviek získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

15.06.2020

CVE

CVE-2020-5754, CVE-2020-5755

Zasiahnuté systémy

Webroot PC Agent verzie staršie ako 9.0.28.48

Následky

Neoprávnený prístup k citlivým údajom
Eskalácia privilégií

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://exchange.xforce.ibmcloud.com/vulnerabilities/183431
https://exchange.xforce.ibmcloud.com/vulnerabilities/183432
https://www.tenable.com/security/research/tra-2020-36

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

Identifikátor

VideoLAN VLC Media Player - zraniteľnosť

Popis

Spoločnosť VideoLAN vydala bezpečnostnú aktualizáciu na svoj video prehrávač VLC Media Player, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť vo funkcii hxxx_AnnexB_to_xVC umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upraveného súboru spôsobiť pretečenie zásobníka a následne vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

17.06.2020

CVE

CVE-2020-13428

Zasiahnuté systémy

VideoLAN VLC Media Player verzie staršie ako 3.0.11

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://www.videolan.org/security/sb-vlc3011.html
https://nvd.nist.gov/vuln/detail/CVE-2020-13428
https://windowsreport.com/vlc-3-crash-bug/

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

Identifikátor

Pulse Secure Desktop Client - zraniteľnosť

Popis

Spoločnosť Pulse Secure vydala bezpečnostnú aktualizáciu na svoje produkty Desktop Client a Installer Service, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť v komponente "dsInstallerService" je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi eskalovať svoje privilégiá.

Dátum prvého zverejnenia varovania

16.06.2020

CVE

CVE-2020-13162

Zasiahnuté systémy

Pulse Secure Desktop Client for Windows verzie staršie ako 9.1R6
Pulse Secure Installer Service for Windows verzie staršie ako 9.1R6

Následky

Eskalácia privilégií

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44503
https://seclists.org/fulldisclosure/2020/Jun/25
https://www.redtimmy.com/privilege-escalation/pulse-secure-client-for-windows-9-1-6-toctou-privilege-escalation-cve-2020-13162/

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

Identifikátor

Drupal CMS - viacero zraniteľností

Popis

Vývojári redakčného systému Drupal vydali bezpečnostné aktualizácie svojho produktu, 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.

Dátum prvého zverejnenia varovania

17.06.2020

CVE

CVE-2020-13663, CVE-2020-13664

Zasiahnuté systémy

Drupal verzie staršie ako 7.72, 8.8.8, 8.9.1 a 9.0.1

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 Drupal v zraniteľných verziách. V prípade že áno, zabezpečte aktualizáciu redakčného systému a zásuvných modulov.
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.drupal.org/sa-core-2020-004
https://www.drupal.org/sa-core-2020-005
https://securityboulevard.com/2020/06/its-time-to-update-your-drupal-now/

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 6.8
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Johnson Controls exacqVision - zraniteľnosť

Popis

Spoločnosť Johnson Controls vydala bezpečnostnú aktualizáciu na svoje produkty, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

18.06.2020

CVE

CVE-2020-9047

Zasiahnuté systémy

Johnson Controls exacqVision Web Service verzie staršie ako 20.06.2.0
Johnson Controls exacqVision Enterprise Manager verzie staršie ako 20.06.3.0

Následky

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

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.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

https://www.johnsoncontrols.com/-/media/jci/cyber-solutions/product-security-advisories/2020/jci-psa-2020-7-v1-exacqvision-web-service-and-enterprise-manager.pdf
https://www.us-cert.gov/ics/advisories/icsa-20-170-01