BEZPEČNOSTNÝ BULLETIN

Týždeň 06. 11. 2019 - 12. 11. 2019

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:
01380/2019/SK-CERT-268

BEZPEČNOSTNÝ BULLETIN

Týždeň 06. 11. 2019 - 12. 11. 2019

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 by mohol vzdialený, neautentifikovaný útočník prostredníctvom zasielania 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

05.11.2019

CVE

CVE-2019-10484, CVE-2019-10485, CVE-2019-10493, CVE-2019-10511, CVE-2019-10545, CVE-2019-10559, CVE-2019-10571, CVE-2019-11833, CVE-2019-2036, CVE-2019-2192, CVE-2019-2193, CVE-2019-2195, CVE-2019-2196, CVE-2019-2197, CVE-2019-2198, CVE-2019-2199, CVE-2019-2201, CVE-2019-2202, CVE-2019-2203, CVE-2019-2204, CVE-2019-2205, CVE-2019-2206, CVE-2019-2207, CVE-2019-2208, CVE-2019-2209, CVE-2019-2211, CVE-2019-2212, CVE-2019-2213, CVE-2019-2214, CVE-2019-2215, CVE-2019-2233, CVE-2019-2288, CVE-2019-2310, CVE-2019-2319, CVE-2019-2320, CVE-2019-2321, CVE-2019-2337, CVE-2019-2338

Zasiahnuté systémy

Operačný systém Android so Security Patch Levels staršími ako 2019-11-05

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/2019-11-01.html
https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-google-android-os-could-allow-for-arbitrary-code-execution_2019-120/

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 aktualizácie na väčšie množstvo svojich produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť v Cisco Small Business RV Series Routers je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

16.10.2019

CVE

CVE-2019-15271, CVE-2019-15276, CVE-2019-15283, CVE-2019-15284, CVE-2019-15285, CVE-2019-15286, CVE-2019-15287, CVE-2019-15288, CVE-2019-15289, CVE-2019-15956, CVE-2019-15957, CVE-2019-15958, CVE-2019-15959, CVE-2019-15960, CVE-2019-15967, CVE-2019-15969, CVE-2019-15973, CVE-2019-15974

Zasiahnuté systémy

Cisco Small Business Routers RV016, RV042, RV042G, and RV082 verzie staršie ako 4.2.3.10 a RV 320 a RV325 verzie staršie ako 1.5.1.05
Cisco Wireless LAN Controller verzie staršie ako 8.10
Cisco PI Software verzie staršie ako 3.4.2, 3.5.1, 3.6.0 Update 02
Cisco EPNM verzie staršie ako 3.0.2.
Cisco TelePresence CE Software verzie staršie ako 9.8.1
Cisco TC Software verzie staršie ako 7.3.19
Cisco RoomOS Software verzie staršie ako RoomOS September Drop 1 2019
Cisco Webex Meetings - Webex Network Recording Player and Webex Player pre Windows verzie staršie ako 39.5.12
Cisco Webex Meetings Online - Webex Network Recording Player and Webex Player pre Windows verzie staršie ako 1.3.44
Cisco Webex Meetings Server - Webex Network Recording Player verzie staršie ako 4.0MR2
Cisco Small Business SPA500 Series IP Phones firmware verzie 7.6.2SR5 a staršie
Cisco MSX verzie staršie ako 3.7.0.
Cisco IND verzie staršie ako 1.7.1-45.

Následky

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

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-20191106-sbrv-cmd-x https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191106-wsa-unauth-devreset https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191106-wlc-dos https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191106-webex-player https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191106-telepres-roomos-privesc https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191106-telepres-roomos-dos https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191106-sbr-cominj https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191106-pi-epn-codex https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191106-wsa-xss https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191106-wbs-privilege https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191106-telece-ros-eve https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191106-spa500-script https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191106-msa-open-redirect https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191106-idn-xss https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-cisco-webex-network-recording-player-and-cisco-webex-player-could-allow-for-arbitrary-code-execution_2019-121/

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

Identifikátor

Honeywell MAXPRO VMS a NVR zraniteľnosti

Popis

Spoločnosť Honeywell vydala bezpečnostné aktualizácie na svoje produkty MAXPRO VMS a NVR, ktoré opravujú viacero bezpečnostných zraniteľností.
Bezpečnostné zraniteľnosti sú spôsobené nedostatočnou implementáciou bezpečnostných mechanizmov a umožňujú vzdialenému, neautentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

25.10.2019

CVE

-

Zasiahnuté systémy

Honeywell MAXPRO VMS verzie staršie ako 560 Build 595 T2-Patch
Honeywell MAXPRO NVR verzie staršie ako 5.6 Build 595 T2-Patch

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.security.honeywell.com/-/media/Security/Resources/PDF/Product-Warranty/Security_Notification_SN_2019-10-25_01-pdf.pdf?la=en-US&hash=39A19559302684C49AC5D74CBC291C9963269DC4

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

Identifikátor

Zraniteľnosti v ovládačoch NVIDIA

Popis

Spoločnosť NVIDIA vydala bezpečnostné aktualizácie na svoje produkty GPU Display Driver a vGPU Software, 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

06.11.2019

CVE

CVE-2019-5690, CVE-2019-5691, CVE-2019-5692, CVE-2019-5693, CVE-2019-5694, CVE-2019-5695, CVE-2019-5696, CVE-2019-5697, CVE-2019-5698

Zasiahnuté systémy

NVIDIA GPU Display Driver verzie staršie ako 441.12
NVIDIA NVIDIA vGPU Software verzie staršie ako 426.26 a 418.109

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/4907
https://exchange.xforce.ibmcloud.com/vulnerabilities/171258

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

Identifikátor

NVIDIA GeForce Experience zraniteľnosti

Popis

Spoločnosť NVIDIA vydala bezpečnostné aktualizácie na svoj produkt GeForce Experience, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšie bezpečnostné zraniteľnosti sú spôsobené nedostatočnou implementáciou bezpečnostných mechanizmov a umožňujú lokálnemu, autentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

06.11.2019

CVE

CVE-2019-5689, CVE-2019-5695, CVE-2019-5701

Zasiahnuté systémy

NVIDIA GeForce Experience verzie staršie ako 3.20.1

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/4860
https://exchange.xforce.ibmcloud.com/vulnerabilities/171253

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

Identifikátor

Fuji Electric V-Server zraniteľnosť

Popis

Spoločnosť Fuji Electric vydala bezpečnostnú aktualizáciu na svoj produkt V-Server, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených VPR súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

07.11.2019

CVE

CVE-2019-18240

Zasiahnuté systémy

Fuji Electric V-Server verzie staršie ako 4.0.7.0

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.
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.us-cert.gov/ics/advisories/icsa-19-311-02
https://www.zerodayinitiative.com/advisories/ZDI-19-971/

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

Identifikátor

Atlassian Jira Service Desk Server a Data Center zraniteľnosti

Popis

Spoločnosť Atlassian vydala bezpečnostnú aktualizáciu na svoje produkty Jira Service Desk Server a Data Center, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup do systému a k citlivým údajom.

Dátum prvého zverejnenia varovania

08.11.2019

CVE

CVE-2019-15003, CVE-2019-15004

Zasiahnuté systémy

Jira Service Desk Server and Data Center verzie staršie ako 3.9.16, 3.16.8, 4.1.3, 4.2.5, 4.3.4, 4.4.1

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnený prístup do 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.

Zdroje

https://jira.atlassian.com/browse/JSDSERVER-6589
https://jira.atlassian.com/browse/JSDSERVER-6590
https://seclists.org/bugtraq/2019/Nov/9
https://exchange.xforce.ibmcloud.com/vulnerabilities/171232
https://exchange.xforce.ibmcloud.com/vulnerabilities/171231
https://packetstormsecurity.com/files/155214/Jira-Service-Desk-Server-Data-Center-Path-Traversal.html

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

Identifikátor

Mitsubishi Electric MELSEC-Q and MELSEC-L zraniteľnosť

Popis

Spoločnosť Mitsubishi Electric vydala bezpečnostnú aktualizáciu na svoje produkty MELSEC-Q a MELSEC-L, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť v CPU module umožňuje vzdialenému, neautentifikovanému útočníkovi spôsobiť zneprístupnenie FTP služieb.

Dátum prvého zverejnenia varovania

07.11.2019

CVE

CVE-2019-13555

Zasiahnuté systémy

Mitsubishi Electric MELSEC-Q and MELSEC-L verzie staršie ako 4.0.7.0

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

https://www.us-cert.gov/ics/advisories/icsa-19-311-01

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

Identifikátor

Honeywell equIP and Recorders zraniteľnosti

Popis

Spoločnosť Honeywell vydala bezpečnostné aktualizácie na svoje IP kamery a rekordéry, ktoré opravujú viacero bezpečnostných zraniteľností.
Bezpečnostné zraniteľnosti sú spôsobené nedostatočnou implementáciou bezpečnostných mechanizmov a umožňujú vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup do systému a spôsobiť zneprístupnenie služieb.

Dátum prvého zverejnenia varovania

13.09.2019

CVE

CVE-2019-18226, CVE-2019-18228, CVE-2019-18230

Zasiahnuté systémy

Honeywell equIP
Honeywell Performance Series Cameras
Honeywell Recorders

Následky

Zneprístupnenie služby
Neoprávnený prístup k citlivým údajom
Neoprávnený prístup do systému

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.security.honeywell.com/-/media/Security/Resources/PDF/Product-Warranty/Security_Notification_SN_2019-09-13-01_V4-pdf.pdf?la=en-US&hash=163378B6E8A4681AF8D753B8CB35F03F2DD147C6
https://www.security.honeywell.com/-/media/Security/Resources/PDF/Product-Warranty/Security_Notification_SN_2019-09-13-02_V4-pdf.pdf?la=en-US&hash=7FDD915D188FB3257E0E712FC6A3E520B45560AB
https://www.security.honeywell.com/-/media/Security/Resources/PDF/Product-Warranty/Security_Notification_SN_2019-09-04-01_V4-pdf.pdf?la=en-US&hash=929A620154F2390954FB4C2A28AC8C1E3B37D008
https://www.us-cert.gov/ics/advisories/icsa-19-304-03
https://www.us-cert.gov/ics/advisories/icsa-19-304-04
https://www.us-cert.gov/ics/advisories/icsa-19-304-02

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

Identifikátor

Amazon Ring Video Doorbell Pro zraniteľnosť

Popis

Spoločnosť Amazon vydala bezpečnostnú aktualizáciu na svoj produkt Ring Video Doorbell Pro, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup k autentifikačným údajom WiFi siete.

Dátum prvého zverejnenia varovania

07.11.2019

CVE

-

Zasiahnuté systémy

Amazon Ring Video Doorbell Pro

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.bitdefender.com/files/News/CaseStudies/study/294/Bitdefender-WhitePaper-RDoor-CREA3949-en-EN-GenericUse.pdf
https://thehackernews.com/2019/11/ring-doorbell-wifi-password.html
https://www.truenorthnetworks.com/blog/amazon-s-ring-video-doorbell-lets-attackers-steal-your-wi-fi-password
https://www.zdnet.com/article/amazon-fixes-ring-video-doorbell-wi-fi-security-vulnerability/