BEZPEČNOSTNÝ BULLETIN

Týždeň 07. 10. 2020 - 13. 10. 2020

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Google Chrome - viacero zraniteľností	Vysoká	**8.8**
02.	Cisco produkty - viacero zraniteľností	Vysoká	**8.8**
03.	Google Android - viacero zraniteľností	Vysoká	**8.8**
04.	ELECOM routre - zraniteľnosť	Vysoká	**8.8**
05.	Mitsubishi Electric MELSEC iQ-R Series	Vysoká	**8.6**
06.	Sympa - zraniteľnosť	Vysoká	**8.4**
07.	Jenkins produkty - viacero zraniteľností	Vysoká	**8.0**
08.	IBM QRadar SIEM - viacero zraniteľností	Vysoká	**7.5**
09.	Realtek rtl81xx SDK Wi-Fi Driver - zraniteľnosti	Vysoká	**7.5**
10.	Apache Fineract, Calcite - zraniteľnosti	Vysoká	**7.5**
11.	KDE Connect - zraniteľnosť	Vysoká	**7.4**
12.	Electron - zraniteľnosť	Vysoká	**7.3**
13.	Atlassian produkty - viacero zraniteľností	Vysoká	**7.2**
14.	Gitlab - viacero zraniteľností	Vysoká	**7.1**
15.	AMD ATIKMDAG.SYS - zraniteľnosť	Vysoká	**7.1**
16.	Johnson Controls victor Web Client - zraniteľnosť	Vysoká	**7.1**

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-246

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 zraniteľnosti by vzdialený neautentifikovaný útočník mohol prostredníctvom podvrhnutia špeciálne upraveného webového obsahu zneužiť na vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

07.10.2020

CVE

CVE-2020-15967, CVE-2020-15968, CVE-2020-15969, CVE-2020-15970, CVE-2020-15971, CVE-2020-15972, CVE-2020-15973, CVE-2020-15974, CVE-2020-15975, CVE-2020-15976, CVE-2020-15977, CVE-2020-15978, CVE-2020-15979, CVE-2020-15980, CVE-2020-15981, CVE-2020-15982, CVE-2020-15983, CVE-2020-15984, CVE-2020-15985, CVE-2020-15986, CVE-2020-15987, CVE-2020-15988, CVE-2020-15989, CVE-2020-15990, CVE-2020-15991, CVE-2020-15992, CVE-2020-6557

Zasiahnuté systémy

Google Chrome verzie staršie ako 86.0.4240.75

Následky

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

Odporúčania

Administrátorom a používateľom 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/2020/10/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

Cisco produkty - viacero zraniteľností

Popis

Spoločnosť Cisco vydala bezpečnostné aktualizácie, ktoré opravujú viacero bezpečnostných zraniteľností.
Zraniteľnosť v IP kamerách Cisco Video Surveillance 8000 Series spočíva v nesprávnej implementácii Cisco Discovery protokolu a neautentifikovaný útočník nachádzajúci sa v rovnakom sieťovom segmente by ju mohol zneužiť na vykonanie škodlivého kódu.
Zraniteľnosť v Cisco Webex Teams spočíva v nesprávnej implementácii mechanizmu načítavania DLL knižníc a lokálny autentifikovaný útočník by ju mohol zneužiť na vykonanie škodlivého kódu.
Zraniteľnosť v Cisco Identity Services Engine spočíva v nedostatočnom vynucovaní RBAC pravidiel vo webovom administratívnom rozhraní a vzdialený autentifikovaný útočník by ju prostredníctvom podvrhnutia špeciálne vytvorených HTTP požiadaviek mohol zneužiť na zmenu konfigurácie systémov a následné zneprístupnenie služby.

Dátum prvého zverejnenia varovania

07.10.2020

CVE

CVE-2020-3467, CVE-2020-3535, CVE-2020-3544

Zasiahnuté systémy

Cisco Video Surveillance 8000 Series IP kamery s firmwarom verzie staršej ako Release 1.0.9-5 s aktivovaným Cisco Discovery Protocol
Cisco Webex Teams pre Windows verzie od 3.0.13464.0 do 3.0.16040.0
Cisco Identity Services Engine Release verzie 2.3 až 2.7

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov a zariadení.
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-cdp-rcedos-mAHR8vNx
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-teams-dll-drsnH5AN
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-auth-bypass-uJWqLTZM

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

05.10.2020

CVE

CVE-2018-11970, CVE-2019-10527, CVE-2019-10596, CVE-2019-10628, CVE-2019-10629, CVE-2019-13992, CVE-2019-13994, CVE-2019-13995, CVE-2019-14074, CVE-2019-14117, CVE-2020-0114, CVE-2020-0215, CVE-2020-0246, CVE-2020-0377, CVE-2020-0378, CVE-2020-0398, CVE-2020-0400, CVE-2020-0404, CVE-2020-0407, CVE-2020-0408, CVE-2020-0410, CVE-2020-0411, CVE-2020-0412, CVE-2020-0413, CVE-2020-0414, CVE-2020-0415, CVE-2020-0416, CVE-2020-0419, CVE-2020-0420, CVE-2020-0421, CVE-2020-11124, CVE-2020-11129, CVE-2020-11133, CVE-2020-3617, CVE-2020-3620, CVE-2020-3621, CVE-2020-3622, CVE-2020-3629, CVE-2020-3634, CVE-2020-3656, CVE-2020-3671

Zasiahnuté systémy

Operačný systém Android so Security Patch Levels staršími ako 2020-10-05

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/2020-10-01
https://security.samsungmobile.com/securityUpdate.smsb

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

Identifikátor

ELECOM routre - zraniteľnosť

Popis

Spoločnosť ELECOM vydala bezpečnostné aktualizácie na routre rady ELECOM WRC, ktoré opravujú bezpečnostnú zraniteľnosť.
Uvedenú zraniteľnosť by neautentifikovaný útočník nachádzajúci sa v rovnakom sieťovom segmente mohol zneužiť na vykonanie škodlivého kódu a získanie úplnej kontroly nad zariadením.

Dátum prvého zverejnenia varovania

05.10.2020

CVE

CVE-2020-5634

Zasiahnuté systémy

ELECOM WRC-2533GST2 s firmwarom verzie 1.13
ELECOM WRC-1900GST2 s firmwarom verzie 1.13
ELECOM WRC-1750GST2 s firmwarom verzie 1.13
ELECOM WRC-1167GST2 s firmwarom verzie1.13

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu 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

http://jvn.jp/en/jp/JVN82892096/index.html
https://exchange.xforce.ibmcloud.com/vulnerabilities/189361

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

Identifikátor

Mitsubishi Electric MELSEC iQ-R Series

Popis

Bezpečnostný výskumníci zverejnili informácie o bezpečnostnej zraniteľnosti v produktoch Mitsubishi MELSEC iQ-R Series.
Bližšie nešpecifikovanú zraniteľnosť by vzdialený neautentifikovaný útočník mohol zneužiť na zneprístupnenie služby.

Dátum prvého zverejnenia varovania

08.10.2020

CVE

CVE-2020-16850

Zasiahnuté systémy

R00/01/02CPU všetky verzie
R04/08/16/32/120(EN)CPU všetky verzie
R08/16/32/120SFCPU všetky verzie
R08/16/32/120PCPU všetky verzie
R16/32/64MTCPU všetky verzie

Následky

Zneprístupnenie služby

Odporúčania

Na uvedenú zraniteľnosť v súčasnosti nie sú dostupné aktualizácie. Administrátorom odporúčame sledovať stránky výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu zasiahnutých systémov.
Administrátorom odporúčame riadiace jednotky a systémy prevádzkovať úplne oddelené od Internetu.

Zdroje

https://us-cert.cisa.gov/ics/advisories/icsa-20-282-02
https://exchange.xforce.ibmcloud.com/vulnerabilities/189571

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.4**
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Sympa - zraniteľnosť

Popis

Bezpečnostní výskumníci upozornili na zraniteľnosť softwaru na správu mailing listov Sympa.
Zraniteľnosť by lokálny neautentifikovaný útočník mohol zneužiť na eskaláciu privilégií na úroveň administrátora a získanie úplnej kontroly nad systémom.

Dátum prvého zverejnenia varovania

07.10.2020

CVE

CVE-2020-26880

Zasiahnuté systémy

Sympa verzie 6.2.57b.2

Následky

Eskalácia privilégií
Neoprávnený prístup k citlivým údajom

Odporúčania

Na uvedenú zraniteľnosť v súčasnosti nie sú dostupné aktualizácie. Administrátorom odporúčame sledovať stránky výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu zasiahnutých systémov.
Zraniteľnosť je možné dočasne eliminovať nahradením sympa_newaliases-wrapper alternatívnym alias manažérom.
Viac informácií nájdete online na https://github.com/sympa-community/sympa/issues/1009.

Zdroje

https://github.com/sympa-community/sympa/issues/1009
https://exchange.xforce.ibmcloud.com/vulnerabilities/189525

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.0**
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Jenkins produkty - viacero zraniteľností

Popis

Spoločnosť Jenkins vydala bezpečnostné aktualizácie, ktoré opravujú viacero zraniteľností vo svojom portfóliu produktov. Najzávažnejšie zraniteľnosti sa nachádzajú v produktoch Jenkins Active Choices Plugin, Jenkins Release Plugin a Jenkins Nerrvana Plugin.
Zraniteľnosti v produktoch Jenkins Active Choices Plugin a Jenkins Release Plugin spočívajú v nedostatočnom spracovaní používateľských vstupov a vzdialený neautentifikovaný útočník by ich mohol zneužiť na realizáciu XSS útokov a získanie prístupu k autentifikačným údajom uloženým v cookies.
Zraniteľnosť v produkte Jenkins Nerrvana Plugin spočíva v nesprávnom spracovaní XXE deklarácií XML parserom a vzdialený autentifikovaný útočník by ju prostredníctvom podvrhnutia špeciálne vytvoreného XML mohol zneužiť na získanie prístupu k citlivým údajom a realizáciu server-side request forgery útokov.

Dátum prvého zverejnenia varovania

08.10.2020

CVE

CVE-2020-2286, CVE-2020-2287, CVE-2020-2288, CVE-2020-2289, CVE-2020-2290, CVE-2020-2291, CVE-2020-2292, CVE-2020-2293, CVE-2020-2294, CVE-2020-2295, CVE-2020-2296, CVE-2020-2297, CVE-2020-2298

Zasiahnuté systémy

Jenkins Role-based Authorization Strategy Plugin 3.0
Jenkins Audit Trail Plugin 3.6
Jenkins Active Choices Plugin 2.4
Jenkins couchdb-statistics Plugin 0.3
Jenkins Release Plugin 2.10.2
Jenkins Persona Plugin 2.4
Jenkins Maven Cascade Release Plugin 1.3.2
Jenkins Shared Objects Plugin 0.44
Jenkins SMS Notification Plugin 1.2
Jenkins Nerrvana Plugin 1.02.06

Následky

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

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.jenkins.io/security/advisory/2020-10-08/

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

Identifikátor

IBM QRadar SIEM - viacero zraniteľností

Popis

Spoločnosť IBM vydala bezpečnostnú aktualizáciu na svoj produkt IBM QRadar SIEM, ktorá opravuje dvojicu bezpečnostných zraniteľností.
Najzávažnejšia zraniteľnosť spočíva v implementačnej chybe autentifikácie prostredníctvom Active Directory a neautentifikovaný útočník nachádzajúci sa v rovnakom sieťovom segmente by ju mohol zneužiť na vykonanie "spoofing" útokov a získanie úplnej kontroly nad systémom.
Druhá zraniteľnosť spočíva v nesprávnej deserializácii používateľských vstupov a vzdialený autentifikovaný útočník by ju prostredníctvom podvrhnutia škodlivého Java objektu mohol zneužiť na vykonanie škodlivého kódu.

Dátum prvého zverejnenia varovania

07.10.2020

CVE

CVE-2019-4545, CVE-2020-4280

Zasiahnuté systémy

IBM QRadar SIEM verzie 7.3.0
IBM QRadar SIEM verzie 7.3.3.Patch.4
IBM QRadar SIEM verzie 7.4.0
IBM QRadar SIEM verzie 7.4.1

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://exchange.xforce.ibmcloud.com/vulnerabilities/165877
https://exchange.xforce.ibmcloud.com/vulnerabilities/176140
https://www.ibm.com/support/pages/node/6344077
https://www.ibm.com/support/pages/node/6344079

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

Identifikátor

Realtek rtl81xx SDK Wi-Fi Driver - zraniteľnosti

Popis

Bezpečnostní výskumníci zverejnili informácie o bezpečnostných zraniteľnostiach v Realtek rtl81xx SDK Wi-Fi ovládači.
Zraniteľnosti spočívajú v nesprávnom spracovaní 802.11 rámcov a neautentifikovaný útočník nachádzajúci sa v rovnakom sieťovom segmente by ich mohol zneužiť na vykonanie škodlivého kódu a získanie kontroly nad systémom.

Dátum prvého zverejnenia varovania

08.10.2020

CVE

-

Zasiahnuté systémy

Realtek rtl81xx SDK Wi-Fi Driver

Následky

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

Odporúčania

Na uvedené zraniteľnosti v súčasnosti nie sú dostupné aktualizácie. Administrátorom a používateľom odporúčame sledovať stránky výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu 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-20-1240/
https://www.zerodayinitiative.com/advisories/ZDI-20-1239/

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

Identifikátor

Apache Fineract, Calcite - zraniteľnosti

Popis

Apache Software Foundation vydala bezpečnostné aktualizácie na svoje produkty Apache Fineract a Apache Calcite, ktoré opravujú bezpečnostné zraniteľnosti.
Zraniteľnosť v Apache Fineract spočíva v nedostatočnom zabezpečení používateľského hesla pri komunikácii so systémom, ktoré je prenášané ako URL parameter a nie prostredníctvom HTTP POST. Vzdialený neautentifikovaný útočník by túto zraniteľnosť mohol zneužiť na získanie používateľských hesiel, prienik do systému a prípravu ďalších útokov.
Bližšie nešpecifikovanú zraniteľnosť v Apache Calcite by vzdialený neautentifikovaný útočník mohol zneužiť na realizáciu man-in-the-middle útokov a získanie neoprávneného prístupu k citlivým údajom.

Dátum prvého zverejnenia varovania

09.10.2020

CVE

CVE-2018-20243, CVE-2020-13955

Zasiahnuté systémy

Apache Fineract verzie 0.4.0-incubating
Apache Fineract verzie 0.5.0-incubating
Apache Fineract verzie 0.6.0-incubating
Apache Fineract verzie 1.0.0
Apache Fineract verzie 1.1.0
Apache Fineract verzie 1.2.0
Apache Fineract verzie 1.3.0
Apache Calcite verzie 0.8 až 1.25

Následky

Neoprávený prístup do systému
Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/189597
https://seclists.org/oss-sec/2020/q4/41
https://exchange.xforce.ibmcloud.com/vulnerabilities/189598
https://seclists.org/oss-sec/2020/q4/40

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.4
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

KDE Connect - zraniteľnosť

Popis

Vývojári produktu KDE Connect vydali bezpečnostnú aktualizáciu, ktorá opravuje bezpečnostnú zraniteľnosť.
Zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a neautentifikovaný útočník nachádzajúci sa v rovnakom sieťovom segmente by ju prostredníctvom zasielania špeciálne vytvorených paketov mohol zneužiť na zneprístupnenie služby.

Dátum prvého zverejnenia varovania

02.10.2020

CVE

CVE-2020-26164

Zasiahnuté systémy

KDE Connect verzie staršie ako 20.08.2

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/189515
https://kde.org/info/security/advisory-20201002-1.txt

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

Identifikátor

Electron - zraniteľnosť

Popis

Vývojári frameworku na tvorbu cross-platform aplikácií Electron vydali bezpečnostnú aktualizáciu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bližšie nešpecifikovanú zraniteľnosť by vzdialený neautentifikovaný útočník prostredníctvom zasielania špeciálne vytvorených požiadaviek mohol zneužiť na eskaláciu privilégií a výkonanie škodlivého kódu.

Dátum prvého zverejnenia varovania

05.10.2020

CVE

CVE-2020-15215

Zasiahnuté systémy

Electron Electron 8.5.1
Electron Electron 9.3.0
Electron Electron 10.1.1
Electron Electron 11.0.0-beta.5

Následky

Vykonanie škodlivého kódu
Eskalácia privilégií

Odporúčania

Odporúčame uistiť sa, či Vaše aplikácie nie sú založené na frameworku Electron. V prípade, že áno, 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://github.com/electron/electron/security/advisories/GHSA-56pc-6jqp-xqj8
https://exchange.xforce.ibmcloud.com/vulnerabilities/189496

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.2
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Atlassian produkty - viacero zraniteľností

Popis

Spoločnosť Atlassian vydala bezpečnostné aktualizácie, ktoré opravujú bezpečnostné zraniteľnosti v produktoch PlantUML for Confluence, Refined Toolkit for Confluence, Linking for Confluence, Countdown Timer for Confluence a Server Status for Confluence.
Zraniteľnosti v týchto produktoch by vzdialený neautentifikovaný útočník mohol zneužiť na realizáciu XSS útokov a získanie prístupu k citlivým údajom uloženým v cookies.

Dátum prvého zverejnenia varovania

09.10.2020

CVE

-

Zasiahnuté systémy

Atlassian PlantUML for Confluence verzie 6.43
Atlassian Refined Toolkit for Confluence verzie 2.2.5
Atlassian Linking for Confluence verzie 5.5.3
Atlassian Countdown Timer for Confluence verzie 1.7.0
Atlassian Server Status for Confluence verzie 1.2.1

Následky

Vykonanie škodlivého kódu
Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli viesť k úniku citlivých údajov, 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://seclists.org/fulldisclosure/2020/Oct/15

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

Identifikátor

Gitlab - viacero zraniteľností

Popis

Vývojári Gitlab vydali bezpečnostnú aktualizáciu, ktorá opravuje viacero bezpečnostných zraniteľností Najzávažnejšia zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a vzdialený autentifikovaný útočník by ju mohol zneužiť na realizáciu XSS útokov a získanie prístupu k citlivým údajom uloženým v cookies.

Dátum prvého zverejnenia varovania

02.10.2020

CVE

CVE-2020-13332, CVE-2020-13333, CVE-2020-13335, CVE-2020-133370, CVE-2020-13342, CVE-2020-13345, CVE-2020-13346

Zasiahnuté systémy

GitLab verzie 12.10 až 12.10.12 (CVE-2020-13337)
GitLab verzie 10.8 až 13.2.9, 13.3.0 až 13.3.6, 13.4.0 až 13.4.1 (CVE-2020-13345)
GitLab verzie 13.1 až 13.2.9, 13.3.0 až 13.3.6, 13.4.0 až 13.4.1 (CVE-2020-13333)
GitLab verzie 11.2 až 13.2.9, 13.3.0 až 13.3.6, 13.4.0 až 13.4.1 (CVE-2020-13346)
GitLab verzie 10.1.0 až 13.2.9, 13.3 až 13.3.6, 13.4 až 13.4.1 (CVE-2020-13342)
GitLab verzie 7.12 až 13.2.9, 13.3.0 až 13.3.6, 13.4.0 až 13.4.1 (CVE-2020-13335)
GitLab verzie 8.6 až 13.2.9, 13.3.0 až 13.3.6, 13.4.0 až 13.4.1 (CVE-2020-13334)
GitLab verzie 8.11.0-rc6 až 3.2.9, 13.3.0 až 13.3.6, 13.4.0 až 13.4.1 (CVE-2020-13332)

Následky

Vykonanie škodlivého kódu
Neoprávnený prístup k citlivým údajom
Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame aktualizovať zasiahnuté systémy.

Zdroje

https://gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-13337.json
https://gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-13345.json
https://gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-13333.json
https://gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-13346.json
https://gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-13342.json
https://gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-13335.json
https://gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-13334.json
https://gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-13332.json

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

Identifikátor

AMD ATIKMDAG.SYS - zraniteľnosť

Popis

Bezpečnostní výskumníci zverejnili informácie o bezpečnostnej zraniteľnosti v AMD ATIKMDAG.SYS. Zraniteľnosť spočíva v implementačnej chybe v rámci D3DKMTCreateAllocation handlera a lokálny neautentifikovaný útočník by ju prostredníctvom špeciálne vytvorenej D3DKMTCreateAllocation API požiadavky mohol zneužiť na zneprístupnenie služby.

Dátum prvého zverejnenia varovania

06.10.2020

CVE

CVE-2020-12911

Zasiahnuté systémy

AMD ATIKMDAG.SYS verzie 26.20.15029.27017

Následky

Zneprístupnenie služby

Odporúčania

Na uvedenú zraniteľnosť v súčasnosti nie sú dostupné aktualizácie. Administrátorom odporúčame sledovať stránku výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/189514
https://talosintelligence.com/vulnerability_reports/TALOS-2020-1119

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

Identifikátor

Johnson Controls victor Web Client - zraniteľnosť

Popis

Vývojári produktu American Dynamics victor Web Client vydali bezpečnostnú aktualizáciu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bližšie nešpecifikovanú zraniteľnosť by neautentifikovaný útočník nachádzajúci sa v rovnakom sieťovom segmente mohol zneužiť na vymazanie súborov zariadenia a následné zneprístupnenie služby.

Dátum prvého zverejnenia varovania

08.10.2020

CVE

CVE-2020-9048

Zasiahnuté systémy

Johnson Controls victor Web Client staršie verzie až 5.4.1 vrátane

Následky

Zneprístupnenie služby

Odporúčania

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

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/189382
https://us-cert.cisa.gov/ics/advisories/icsa-20-282-01
https://www.johnsoncontrols.com/-/media/jci/cyber-solutions/product-security-advisories/2020/jci-psa-2020-09-v1-victor-web-client.pdf