BEZPEČNOSTNÝ BULLETIN

Týždeň 01. 09. 2021 - 07. 09. 2021

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Pluginy pre nástroj Jenkins - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
02.	Amazon Kindle e-reader - bezpečnostná zraniteľnosť	Vysoká	**8.4**
03.	Mautic produkt - bezpečnostná zraniteľnosť	Vysoká	**8.2**
04.	WhatsApp produkt - bezpečnostná zraniteľnosť	Vysoká	**7.8**
05.	Samsung Drive Manager - bezpečnostná zraniteľnosť	Vysoká	**7.7**
06.	Linphone Session Initiation Protocol (SIP) - bezpečnostná zraniteľnosť	Vysoká	**7.5**
07.	Redux Gutenberg Template plugin pre WordPress - dve bezpečnostné zraniteľnosti	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-544

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

Identifikátor

Pluginy pre nástroj Jenkins - viacero bezpečnostných zraniteľností

Popis

Vývojári nástroja Jenkins vydali bezpečnostné aktualizácie na zásuvné moduly, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne vytvorenej požiadavky, vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

31.08.2021

CVE

CVE-2021-21677, CVE-2021-21678, CVE-2021-21679, CVE-2021-21680, CVE-2021-21681

Zasiahnuté systémy

Azure AD Plugin vo verzii staršej ako 180.v8b1e80e6f242
Code Coverage API Plugin vo verzii staršej ako 1.4.1
Nested View Plugin vo verzii staršej ako 1.21
Nomad Plugin vo verzii staršej ako 0.7.5
SAML Plugin vo verzii staršej ako 2.0.8

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Odporúčame uistiť sa, či Vaše aplikácie nevyužívajú frameworky, knižnice, pluginy, SDK alebo moduly v zraniteľnej verzii. V prípade, že áno, zabezpečte aktualizáciu všetkých komponentov, od ktorých závisí vaša aplikácia, na aktuálne verzie bez známych bezpečnostných zraniteľností.
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://www.jenkins.io/security/advisory/2021-08-31/
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21679
https://exchange.xforce.ibmcloud.com/vulnerabilities/208472

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

Identifikátor

Amazon Kindle e-reader - bezpečnostná zraniteľnosť

Popis

Spoločnosť Amazon vydala bezpečnostnú aktualizáciu na produkt Kindle E-reader, ktorá opravuje bezpečnostnú zraniteľnosť. Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi eskalovať svoje privilégiá a následne vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

02.09.2021

CVE

CVE-2021-30355

Zasiahnuté systémy

Amazon Kindle E-reader vo verzii staršej ako 5.13.5

Následky

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

Odporúčania

Administrátorom a používateľom 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.
Administrátorom odporúčame limitovať prístup k administratívnemu rozhraniu a jeho funkciám zavedením zoznamu pre riadenie prístupov (ACL).

Zdroje

https://www.amazon.com/Amazon-Kindle-Ereader-Family/b?ie=UTF8&node=6669702011
https://research.checkpoint.com/2021/i-can-take-over-your-kindle/
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30355
https://exchange.xforce.ibmcloud.com/vulnerabilities/208675

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

Identifikátor

Mautic produkt - bezpečnostná zraniteľnosť

Popis

Vývojári nástroja Mautic vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom injekcie škodlivého skriptu, získať neoprávnený prístup k citlivým údajom a vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

01.09.2021

CVE

CVE-2021-27910

Zasiahnuté systémy

Mautic vo verzii staršej ako 3.3.4
Mautic vo verzii staršej ako 4.0.0

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť získanie prístupu k citlivým údajom je dobrou praxou 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.
Pri webových stránkach odporúčame zvážiť možnosť prevádzkovať redakčný systém nedostupný z verejného internetu a na verejný prezentačný server nahrávať len vyexportovanú statickú verziu stránky.

Zdroje

https://github.com/mautic/mautic/security/advisories/GHSA-86pv-95mj-7w5f
https://www.mautic.org/
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27910
https://exchange.xforce.ibmcloud.com/vulnerabilities/208677

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

Identifikátor

WhatsApp produkt - bezpečnostná zraniteľnosť

Popis

Vývojári aplikácie WhatsApp vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvoreného súboru, získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

02.09.2021

CVE

CVE-2020-1910

Zasiahnuté systémy

WhatsApp pre Android vo verzii staršej ako v2.21.1.13
WhatsApp Business pre Android vo verzii staršej ako v2.21.1.13

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme
Zneprístupnenie služby

Odporúčania

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

Zdroje

https://thehackernews.com/2021/09/whatsapp-photo-filter-bug-could-have.html
https://www.cybersafe.news/whatsapp-photo-filter-bug-could-have-led-to-user-data-exposure/
https://research.checkpoint.com/2021/now-patched-vulnerability-in-whatsapp-could-have-led-to-data-exposure-of-users/
https://nvd.nist.gov/vuln/detail/CVE-2020-1910

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.7
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Samsung Drive Manager - bezpečnostná zraniteľnosť

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnosti produktu Samsung Drive Manager. Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi získať neoprávnený prístup k citlivým údajom a vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

01.09.2021

CVE

CVE-2021-39373

Zasiahnuté systémy

Samsung Drive Manager vo verzii staršej ako 2.0.104 (vrátane)

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme

Odporúčania

Na uvedenú zraniteľnosť v súčasnosti nebola vydaná bezpečnostná záplata, administrátorom preto odporúčame sledovať stránku výrobcu a po vydaní bezpečnostných záplat bezodkladne vykonať aktualizáciu zasiahnutých systémov.
Detailné inštrukcie môžete nájsť na webovej adrese:
https://github.com/bosslabdcu/Vulnerability-Reporting/security/advisories/GHSA-j3f7-346q-97f4
Po odstránení zraniteľností, ktoré mohli spôsobiť získanie prístupu k citlivým údajom je dobrou praxou zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.
Administrátorom odporúčame limitovať prístup k administratívnemu rozhraniu a jeho funkciám zavedením zoznamu pre riadenie prístupov (ACL).

Zdroje

https://github.com/bosslabdcu/Vulnerability-Reporting/security/advisories/GHSA-j3f7-346q-97f4
https://www.samsung.com/us/
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39373
https://exchange.xforce.ibmcloud.com/vulnerabilities/208636

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

Identifikátor

Linphone Session Initiation Protocol (SIP) - bezpečnostná zraniteľnosť

Popis

Vývojári klienta Linphone vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne vytvorenej požiadavky, spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

01.09.2021

CVE

CVE-2021-33056

Zasiahnuté systémy

Linphone belle-sip vo verzii staršej ako 4.5.20

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://thehackernews.com/2021/09/linphone-sip-stack-bug-could-let.html
https://nvd.nist.gov/vuln/detail/CVE-2021-33056
https://github.com/BelledonneCommunications/belle-sip/releases/tag/4.5.20

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

Identifikátor

Redux Gutenberg Template plugin pre WordPress - dve bezpečnostné zraniteľnosti

Popis

Vývojári pluginu Redux Gutenberg Template Library & Redux Framework vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii mechanizmov autentifikácie a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zasielania špeciálne vytvorenej požiadavky, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

01.09.2021

CVE

CVE-2021-38312, CVE-2021-38314

Zasiahnuté systémy

Redux Gutenberg Template Library & Redux Framework plugin pre WordPress vo verzii staršej ako 4.2.13

Následky

Neoprávnená zmena v systéme
Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Pri webových stránkach odporúčame zvážiť možnosť prevádzkovať redakčný systém nedostupný z verejného internetu a na verejný prezentačný server nahrávať len vyexportovanú statickú verziu stránky.

Zdroje

https://www.wordfence.com/blog/2021/09/over-1-million-sites-affected-by-redux-framework-vulnerabilities/
https://threatpost.com/gutenberg-template-library-redux-bugs-wordpress/169111/
https://redux.io/
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38312
https://exchange.xforce.ibmcloud.com/vulnerabilities/208687