BEZPEČNOSTNÝ BULLETIN

Týždeň 18. 11. 2020 - 24. 11. 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-275

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

Identifikátor

Zraniteľnosť knižnice musl libc

Popis

Vývojári knižnice musl libc zverejnili informácie o bezpečnostnej zraniteľnosti.
Bezpečnostná zraniteľnosť umožňuje vzdialenému, neautentifikovanému útočníkovi spôsobiť pretečenie zásobníka a následne vykonať škodlivý kód.

Dátum prvého zverejnenia varovania

24.11.2020

CVE

CVE-2020-28928

Zasiahnuté systémy

musl libc všetky verzie staršie ako 1.2.1 (vrátane)

Následky

Vykonanie škodlivého kódu

Odporúčania

Odporúčame uistiť sa, či Vaše aplikácie nevyužívajú danú knižnicu. V prípade, že áno, administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľnosti, ktoré mohli spôsobiť vzdialené vykonanie kódu alebo únik citlivých informácií, 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.openwall.com/lists/musl/2020/11/19/1

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 8.5
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Bezpečnostná zraniteľnosť Drupal

Popis

Vývojári redakčného systému Drupal vydali aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

19.11.2020

CVE

CVE-2020-13671

Zasiahnuté systémy

Drupal 7 verzie staršie ako 7.74
Drupal 8 verzie staršie ako 8.8.11
Drupal 8 verzie staršie ako 8.9.9
Drupal 9 verzie staršie ako 9.0.8.

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľnosti, 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.drupal.org/sa-core-2020-012
https://www.cybersecurity-help.cz/vdb/SB2020111904
https://www.securityweek.com/remote-code-execution-vulnerability-patched-drupal

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

Identifikátor

Zraniteľnosti v LiquidFiles

Popis

Spoločnosť LiquidFiles vydala bezpečnostnú aktualizáciu na svoj systém na odosielanie a prímanie súborov LiquidFiles, ktorá opravuje dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť je spôsobená nedostatočným overovaním používateľských vstupov a umožňuje vzdialenému, autentifikovanému útočníkovi vykonať škodlivý kód a získať prístup k citlivým informáciám.

Dátum prvého zverejnenia varovania

24.11.2020

CVE

CVE-2020-29071, CVE-2020-29072

Zasiahnuté systémy

LiquidFiles Virtual Appliance verzie staršie ako 3.3.19

Následky

Vykonanie škodlivého kódu
Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľnosti, ktoré mohli spôsobiť vzdialené vykonanie kódu alebo únik citlivých informácií, 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://x2f.me/liquidfiles_advisory

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

Identifikátor

Zraniteľnosť Fuji Electric V-Server Lite

Popis

Spoločnosť Fuji Electric vydala bezpečnostnú aktualizáciu na svoj produkt V-Server Lite, ktorá opravuje bezpečnostnú zraniteľnosť.
Zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

24.11.2020

CVE

CVE-2020-25171

Zasiahnuté systémy

V-Server Lite všetky verzie staršie ako 3.3.24.0

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľnosti, 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/ics/advisories/icsa-20-329-02

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

Identifikátor

Zraniteľnosť Mitsubishi Electric MELSEC iQ-R Series

Popis

Spoločnosť Mitsubishi Electric vydala bnezpečnostné aktualizácie na svoj modul MELSEC iQ-R, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvoreného SLMP packetu spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

20.11.2020

CVE

CVE-2020-5668

Zasiahnuté systémy

Mitsubishi Electric MELSEC iQ-R R00/01/02CPU verzie staršie ako 20
Mitsubishi Electric MELSEC iQ-R R04/08/16/32/120 (EN) CPU verzie staršie ako 52
Mitsubishi Electric MELSEC iQ-R R08/16/32/120SFCPU verzie staršie ako 23
Mitsubishi Electric MELSEC iQ-R RJ71EN71 verzie staršie ako 48
Mitsubishi Electric MELSEC iQ-R RJ71GF11-T2 verzie staršie ako 48
Mitsubishi Electric MELSEC iQ-R RJ72GF15-T2 verzie staršie ako 08
Mitsubishi Electric MELSEC iQ-R RJ71GP21-SX verzie staršie ako 48
Mitsubishi Electric MELSEC iQ-R RJ71GP21S-SX verzie staršie ako 48

Následky

Zneprístupnenie služby

Odporúčania

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

Zdroje

https://us-cert.cisa.gov/ics/advisories/icsa-20-324-05

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

Identifikátor

Zraniteľnosť v MongoDB Server

Popis

Spoločnosť MongoDB vydala bezpečnostnú aktualizáciu na svoj produkt MongoDB Server, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej správy spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

24.11.2020

CVE

CVE-2019-20925

Zasiahnuté systémy

MongoDB Server v4.2 verzie staršie ako 4.2.1
MongoDB Server v4.0 verzie staršie ako 4.0.13
MongoDB Server v3.6 verzie staršie ako 3.6.15
MongoDB Server v3.4 verzie staršie ako 3.4.24.

Následky

Zneprístupnenie služby

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.

Zdroje

https://jira.mongodb.org/browse/SERVER-43751

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

Identifikátor

Zraniteľnosť Jupyter server

Popis

Spoločnosť Jupyter Server vydala bezpečnostnú aktualizáciu na svoj produkt Jupyter server, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

24.11.2020

CVE

CVE-2020-26232

Zasiahnuté systémy

Jupyter server verzie staršie ako 1.0.6

Následky

Neoprávnená zmena v systéme

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.

Zdroje

https://github.com/jupyter-server/jupyter_server/blob/master/CHANGELOG.md#106---2020-11-18
https://github.com/jupyter-server/jupyter_server/security/advisories/GHSA-grfj-wjv9-4f9v