BEZPEČNOSTNÝ BULLETIN

Týždeň 02. 09. 2020 - 08. 09. 2020

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Jenkins plugins - viacero zraniteľností	Vysoká	**8.8**
02.	Foxit PhantomPDF - viacero zraniteľností	Vysoká	**8.8**
03.	IBM Aspera Connect - zraniteľnosť	Vysoká	**8.2**
04.	Golang Go - zraniteľnosť	Vysoká	**7.5**
05.	vBulletin - zero-day zraniteľnosti	Vysoká	**7.2**

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-216

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

Identifikátor

Jenkins plugins - viacero zraniteľností

Popis

Vývojári produktu Jenkins informovali o bezpečnostných zraniteľnostiach vo viacerých zásuvných moduloch.
Najzávažnejšie bezpečnostné zraniteľnosti sú spôsobené nedostatočnou implementáciou bezpečnostných mechanizmov a 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

01.09.2020

CVE

CVE-2020-2238, CVE-2020-2239, CVE-2020-2240, CVE-2020-2241, CVE-2020-2242, CVE-2020-2243, CVE-2020-2244, CVE-2020-2245, CVE-2020-2246, CVE-2020-2247, CVE-2020-2248, CVE-2020-2249, CVE-2020-2250, CVE-2020-2251

Zasiahnuté systémy

Build Failure Analyzer Plugin verzie staršie ako 1.27.1
Cadence vManager Plugin verzie staršie ako 3.0.5
database Plugin verzie staršie ako 1.7
Git Parameter Plugin verzie staršie ako 0.9.13
Parameterized Remote Trigger Plugin verzie staršie ako 3.1.4
SoapUI Pro Functional Testing Plugin verzie staršie ako 1.4
JSGames Plugin 0.2 a staršie
Klocwork Analysis Plugin 2020.2.1 a staršie
Team Foundation Server Plugin 5.157.1 a staršie
Valgrind Plugin 0.28 a staršie

Následky

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

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-216

Zdroje
https://www.jenkins.io/security/advisory/2020-09-01/#SECURITY-1831
https://nvd.nist.gov/vuln/detail/CVE-2020-2247
https://nvd.nist.gov/vuln/detail/CVE-2020-2246
https://nvd.nist.gov/vuln/detail/CVE-2020-2245
https://nvd.nist.gov/vuln/detail/CVE-2020-2244
https://nvd.nist.gov/vuln/detail/CVE-2020-2243
https://www.openwall.com/lists/oss-security/2020/09/01/3

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

Identifikátor

Foxit PhantomPDF - viacero zraniteľností

Popis

Spoločnosť Foxit Software vydala bezpečnostnú aktualizáciu na svoj produkt Foxit PhantomPDF, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšie 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

31.08.2020

CVE

CVE-2020-11493, CVE-2020-12247, CVE-2020-12248, CVE-2020-15637, CVE-2020-15638

Zasiahnuté systémy

Foxit PhantomPDF verzie staršie ako 9.7.3

Následky

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

Odporúčania

Administrátorom 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 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.foxitsoftware.com/support/security-bulletins.html
https://nvd.nist.gov/vuln/detail/CVE-2020-12247
https://nvd.nist.gov/vuln/detail/CVE-2020-12248
https://nvd.nist.gov/vuln/detail/CVE-2020-11493

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

Identifikátor

IBM Aspera Connect - zraniteľnosť

Popis

Spoločnosť IBM vydala bezpečnostnú aktualizáciu na svoj produkt Aspera Connect, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

01.09.2020

CVE

CVE-2020-4545

Zasiahnuté systémy

IBM Aspera Connect verzie staršie ako 3.10.0

Následky

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

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.ibm.com/support/pages/node/6326537
https://exchange.xforce.ibmcloud.com/vulnerabilities/183190

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

Identifikátor

Golang Go - zraniteľnosť

Popis

Vývojári jazyka Go vydali bezpečnostnú aktualizáciu, ktorá opravuje bezpečnostnú zraniteľnosť. Bezpečnostná zraniteľnosť je spôsobená nedostatočným overovaním používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom XSS útoku získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

02.09.2020

CVE

CVE-2020-24553

Zasiahnuté systémy

Golang Go verzie staršie ako 1.14.8 a 1.15.1

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://exchange.xforce.ibmcloud.com/vulnerabilities/187776
https://seclists.org/fulldisclosure/2020/Sep/5
https://www.redteam-pentesting.de/en/advisories/rt-sa-2020-004/-inconsistent-behavior-of-gos-cgi-and-fastcgi-transport-may-lead-to-cross-site-scripting

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

Identifikátor

vBulletin - zero-day zraniteľnosti

Popis

Bezpečnostný výskumník informoval o viacerých zero-day bezpečnostných zraniteľnostiach v diskusnom fóre vBulletin.
Bezpečnostné zraniteľnosti sú spôsobené nedostatočným overovaním používateľských vstupov a umožňujú vzdialenému, neautentifikovanému útočníkovi prostredníctvom XSS útoku získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

02.09.2020

CVE

CVE-2020-25115, CVE-2020-25116, CVE-2020-25117, CVE-2020-25118, CVE-2020-25119, CVE-2020-25120, CVE-2020-25121, CVE-2020-25122, CVE-2020-25123, CVE-2020-25124

Zasiahnuté systémy

vBulletin 5.6.4

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Bezpečnostná aktualizácia riešiaca uvedené zraniteľnosti doposiaľ nebola vydaná. Odporúčame sledovať stránky výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu.
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://pentest-vincent.blogspot.com/2020/09/vbulletin-563-multiple-persistent-cross.html
https://exchange.xforce.ibmcloud.com/vulnerabilities/187775
https://exchange.xforce.ibmcloud.com/vulnerabilities/187777
https://exchange.xforce.ibmcloud.com/vulnerabilities/187778
https://exchange.xforce.ibmcloud.com/vulnerabilities/187779
https://exchange.xforce.ibmcloud.com/vulnerabilities/187780
https://exchange.xforce.ibmcloud.com/vulnerabilities/187782
https://exchange.xforce.ibmcloud.com/vulnerabilities/187783
https://exchange.xforce.ibmcloud.com/vulnerabilities/187790
https://exchange.xforce.ibmcloud.com/vulnerabilities/187791

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-216