BEZPEČNOSTNÝ BULLETIN

Týždeň 01. 04. 2020 - 07. 04. 2020

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	WordPress Plugin for Auth0 viacero zraniteľností	Vysoká	**8.8**
02.	NGINX Controller zraniteľnosť	Vysoká	**8.6**
03.	Avast Antivirus zraniteľnosti	Vysoká	**8.4**
04.	Apache HTTP Server a Druid viacero zraniteľností	Vysoká	**8.1**

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-078

BEZPEČNOSTNÝ BULLETIN

Týždeň 01. 04. 2020 - 07. 04. 2020

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

Identifikátor

WordPress Plugin for Auth0 viacero zraniteľností

Popis

Vývojári WordPress Plugin for Auth0 vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje viacero bezpečnostných zraniteľností.
Bezpečnostné zraniteľnosti sú spôsobené nedostatočným overovaním používateľských vstupov 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

31.03.2020

CVE

CVE-2020-5391, CVE-2020-5392, CVE-2020-6753, CVE-2020-7947, CVE-2020-7948

Zasiahnuté systémy

WordPress Plugin for Auth0 verzie staršie ako 4.0.0

Následky

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

Odporúčania

Odporúčame uistiť sa, či Vaše webové stránky nie sú založené na redakčnom systéme Wordpress so zraniteľnou verziou pluginu. V prípade že áno, zabezpečte aktualizáciu redakčného systému a pluginu.
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://auth0.com/docs/security/bulletins/2020-03-31_wpauth0
https://github.com/auth0/wp-auth0/security/advisories/GHSA-59vf-cgfw-6h6v

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

Identifikátor

NGINX Controller zraniteľnosť

Popis

Vývojári NGINX Controller vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov v Controller API a umožňuje vzdialenému, autentifikovanému útočníkovi eskalovať svoje privilégiá na zasiahnutom systéme a spôsobiť zneprístupnenie služieb.

Dátum prvého zverejnenia varovania

26.03.2020

CVE

CVE-2020-5863

Zasiahnuté systémy

NGINX Controller verzie staršie ako 3.2.0

Následky

Zneprístupnenie služby
Eskalácia privilégií

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://support.f5.com/csp/article/K14631834
https://nvd.nist.gov/vuln/detail/CVE-2020-5863

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

Identifikátor

Avast Antivirus zraniteľnosti

Popis

Spoločnosť Avast vydala bezpečnostnú aktualizáciu na svoj produkt Avast Antivirus, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšie bezpečnostné zraniteľnosti umožňujú lokálnemu, neautentifikovanému útočníkovi eskalovať svoje privilégiá a vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

02.04.2020

CVE

CVE-2020-10860, CVE-2020-10861, CVE-2020-10862, CVE-2020-10863, CVE-2020-10864, CVE-2020-10865, CVE-2020-10866, CVE-2020-10867, CVE-2020-10868

Zasiahnuté systémy

Avast Antivirus verzie staršie ako 20.2.2401

Následky

Eskalácia privilégií
Neoprávnená zmena v systéme
Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://github.com/umarfarook882/Avast_Multiple_Vulnerability_Disclosure/blob/master/README.md
https://forum.avast.com/index.php?topic=232420.0
https://forum.avast.com/index.php?topic=232423.0
https://nvd.nist.gov/vuln/detail/CVE-2020-10860
https://exchange.xforce.ibmcloud.com/vulnerabilities/178945
https://exchange.xforce.ibmcloud.com/vulnerabilities/178944

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

Identifikátor

Apache HTTP Server a Druid viacero zraniteľností

Popis

Spoločnosť Apache vydala bezpečnostné aktualizácie na svoje produkty HTTP Server a Druid , ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšie bezpečnostné zraniteľnosti umožňujú vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup do systému a následne vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

01.03.2020

CVE

CVE-2020-1927, CVE-2020-1934, CVE-2020-1958

Zasiahnuté systémy

Apache Druid verzie staršie ako 0.17.1
Apache Apache HTTP Server verzie staršie ako 2.4.43

Následky

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

Odporúčania

Administrátorom zasiahnutých systémov odporúčame bezodkladne nainštalovať bezpečnostné aktualizácie.
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://downloads.apache.org/httpd/CHANGES_2.4.43
https://exchange.xforce.ibmcloud.com/vulnerabilities/178936
https://exchange.xforce.ibmcloud.com/vulnerabilities/178937
https://exchange.xforce.ibmcloud.com/vulnerabilities/178939
https://seclists.org/oss-sec/2020/q2/5
https://lists.apache.org/thread.html/r9d437371793b410f8a8e18f556d52d4bb68e18c537962f6a97f4945e%40%3Cdev.druid.apache.org%3E