NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

BEZPEČNOSTNÉ VAROVANIE

No: V20200604-01K

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☐ **Vysoká**	☒ **Kritická**	**CVSS skóre: 9.8**
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Apache Tomcat zraniteľnosť

Popis

Spoločnosť Apache vydala bezpečnostné aktualizácie na svoj produkt Tomcat, ktoré opravujú kritickú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť v komponente PersistentManager umožňuje vzdialenému, neautentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému. Na uvedenú zraniteľnosť je v súčasnosti voľne dostupný Proof-of-Concept kód.

Dátum prvého zverejnenia varovania

30.05.2020

CVE

CVE-2019-17569, CVE-2020-1935, CVE-2020-1938

Zasiahnuté systémy

Apache Tomcat verzie staršie ako 10.0.0-M5, 9.0.35, 8.5.55 a 7.0.104

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://seclists.org/fulldisclosure/2020/Jun/6
https://www.redtimmy.com/java-hacking/apache-tomcat-rce-by-deserialization-cve-2020-9484-write-up-and-exploit/
https://nvd.nist.gov/vuln/detail/CVE-2020-9484

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-135