



NCSC-2025-0089

Kwetsbaarheid verholpen in Apache Tomcat

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 17-03-2025

TLP:WHITE

Toegestane verspreiding van TLP:WHITE

(Traffic Light Protocol)

Deze handreiking bevat het label TLP:WHITE en wordt door het NCSC verspreid. Het NCSC gebruikt het Traffic Light Protocol (TLP) om eenduidig te definiëren wat er met de informatie mag gebeuren. Wanneer informatie is voorzien van een TLP-aanduiding weet u met wie u deze informatie mag delen. Dit staat beschreven in de standaard First (www.first.org/tlp).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op info@ncsc.nl

Feiten

Apache heeft een kwetsbaarheid verholpen in Apache Tomcat (Specifiek voor versies 11.0.0-M1 tot 11.0.2, 10.1.0-M1 tot 10.1.34, en 9.0.0.M1 tot 9.0.98).

Duiding

De kwetsbaarheid bevindt zich in de manier waarop de server omgaat met HTTP PUT-verzoeken. Door een kwaadaardig PUT-verzoek te sturen, kan een aanvaller willekeurige bestanden uploaden en uiteindelijk remote code execution (RCE) verkrijgen. Dit stelt hen in staat om volledige controle over de server te krijgen. Deze kwetsbaarheid wordt momenteel actief misbruikt in aanvallen, wat de urgentie van het aanpakken van dit beveiligingsprobleem in getroffen implementaties onderstreept.

Oplossingen

Apache heeft updates uitgebracht om de kwetsbaarheid te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

➤ <https://www.cve.org/CVERecord?id=CVE-2025-24813>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2025-24813	8.7 HIGH

CWE's

CWE	Beschrijving
➤ CWE-44	Path Equivalence: 'file.name' (Internal Dot)
➤ CWE-444	Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling')
➤ CWE-502	Deserialization of Untrusted Data

Getroffen producten

Red Hat
tomcat
pki-servlet-engine
tomcat6
Red Hat Enterprise Linux 8
SUSE
SUSE openSUSE
Apache
Tomcat
Apache Software Foundation
Apache Tomcat
Debian
tomcat10
tomcat9

Disclaimer

The Netherlands Cyber Security Center (henceforth: NCSC-NL) maintains this page to enhance access to its information and security advisories. The use of this security advisory is subject to the following terms and conditions: NCSC-NL makes every reasonable effort to ensure that the content of this page is kept up to date, and that it is accurate and complete. Nevertheless, NCSC-NL cannot entirely rule out the possibility of errors, and therefore cannot give any warranty in respect of its completeness, accuracy or continuous keeping up-to-date. The information contained in this security advisory is intended solely for the purpose of providing general information to professional users. No rights can be derived from the information provided therein. NCSC-NL and the Kingdom of the Netherlands assume no legal liability or responsibility for any damage resulting from either the use or inability of use of this security advisory. This includes damage resulting from the inaccuracy of incompleteness of the information contained in the advisory. This security advisory is subject to Dutch law. All disputes related to or arising from the use of this advisory will be submitted to the competent court in The Hague. This choice of means also applies to the court in summary proceedings.