



NCSC-2025-0195

Kwetsbaarheden verholpen in Apache Tomcat

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 18-06-2025

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 kwetsbaarheden verholpen in Apache Tomcat (Specifiek voor versies 11.0.0-M1 tot 11.0.7, 10.1.0-M1 tot 10.1.41, en 9.0.0-M1 tot 9.0.105).

Duiding

De kwetsbaarheden omvatten een denial-of-service door onvoldoende limieten op multipart headers, een gebrek aan resource allocatie zonder limieten, een onbetrouwbaar zoekpad in de Windows installer, en een kritieke authenticatie omzeiling door onjuiste padverwerking. Aanvallers kunnen deze kwetsbaarheden misbruiken door speciaal samengestelde verzoeken te sturen, wat kan leiden tot ongeoorloofde toegang tot gevoelige bestanden en geheugenuitputting, met als gevolg een verstoring van de service.

Oplossingen

Apache heeft updates uitgebracht om de kwetsbaarheden te verhelpen, waaronder upgrades naar versies 11.0.8, 10.1.42, of 9.0.106. Zie bijgevoegde referenties voor meer informatie.

Referenties

- <https://tomcat.apache.org/security-10.html>
- <https://tomcat.apache.org/security-11.html>
- <https://tomcat.apache.org/security-9.html>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2025-48976	8.7 HIGH
➤ CVE-2025-48988	8.7 HIGH
➤ CVE-2025-49124	7.3 HIGH
➤ CVE-2025-49125	6.9 MEDIUM

CWE's

CWE	Beschrijving
> CWE-426	Untrusted Search Path
> CWE-404	Improper Resource Shutdown or Release
> CWE-770	Allocation of Resources Without Limits or Throttling
> CWE-288	Authentication Bypass Using an Alternate Path or Channel

Getroffen producten

Apache Software Foundation
Apache Tomcat

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.