



NCSC-2025-0337

Kwetsbaarheden verholpen in Oracle Java

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 23-10-2025

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

Oracle heeft kwetsbaarheden verholpen in Oracle Java SE en Oracle GraalVM (Specifiek voor versies 21.0.8 en 25 van Oracle Java SE, en versie 21.3.15 van Oracle GraalVM Enterprise Edition).

Duiding

De kwetsbaarheden stellen ongeauthenticeerde aanvallers met netwerktoegang in staat om systemen te compromitteren, wat kan leiden tot ongeautoriseerde gegevensmanipulatie en het risico op datalekken. De ernst van deze kwetsbaarheden wordt onderstreept door CVSS-scores variërend van 3.1 tot 7.5, wat wijst op aanzienlijke risico's voor de integriteit en vertrouwelijkheid van gegevens. De kwetsbaarheden zijn aanwezig in verschillende versies van de software, wat de noodzaak van updates benadrukt.

Oplossingen

Oracle heeft updates uitgebracht om de kwetsbaarheden te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

➤ <https://www.oracle.com/security-alerts/cpuoct2025.html>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2025-31257	8.8 HIGH
➤ CVE-2025-53057	5.9 MEDIUM
➤ CVE-2025-53066	7.5 HIGH
➤ CVE-2025-61748	3.7 LOW
➤ CVE-2025-61755	3.7 LOW

CWE's

CWE	Beschrijving
> CWE-20	Improper Input Validation
> CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer
> CWE-200	Exposure of Sensitive Information to an Unauthorized Actor
> CWE-284	Improper Access Control
> CWE-416	Use After Free
> CWE-862	Missing Authorization

Getroffen producten

Oracle
Java Se
Oracle GraalVM Enterprise Edition
Oracle GraalVM for JDK

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.