



Advisory NCSC-2026-0449

PRIORITEIT: NORMAAL

Meerdere kwetsbaarheden verholpen in Oracle Java

Publicatiedatum: 22-10-2026

Toegestane verspreiding: TLP:WHITE
(Traffic Light Protocol)

Deze publicatie bevat het label TLP:WHITE en wordt door het Nationaal Cyber Security Center (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.

Reacties zijn welkom op info@ncsc.nl.

Feiten

Oracle heeft meerdere kwetsbaarheden verholpen in Oracle Java.

Duiding

In Oracle Java SE, JavaFX en GraalVM Enterprise Edition zijn diverse kwetsbaarheden aanwezig die door ongeauthenticeerde netwerkaanvallers kunnen worden misbruikt via blootgestelde API's of sandboxed Java-applicaties.

Deze kwetsbaarheden maken het mogelijk om denial of service te veroorzaken, ongeautoriseerde lees- en schrijfacties op data uit te voeren, en in sommige gevallen beperkte data toegang te verkrijgen. Exploitatie kan plaatsvinden via netwerktoegang, soms met vereiste van gebruikersinteractie, en betreft meerdere componenten zoals de compiler, networking, JAXP, JDBC, RMI, ImageIO, Lightweight HTTP Server en CORBA. Daarnaast zijn er kwetsbaarheden die leiden tot crashes of het vastlopen van systemen bij het uitvoeren van onbetrouwbare code in sandboxed omgevingen.

Oplossingen

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

Referenties

- <https://www.oracle.com/security-alerts/cpuoct2026.html>

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-6732	7.5 HIGH
CVE-2026-43660	7.5 HIGH
CVE-2026-46470	9.1 CRITICAL
CVE-2026-83374	5.9 MEDIUM

CVE	CVSS Score
CVE-2026-83376	3.7 LOW
CVE-2026-83378	4.8 MEDIUM
CVE-2026-83380	5.3 MEDIUM
CVE-2026-83381	4.8 MEDIUM
CVE-2026-83387	5.9 MEDIUM
CVE-2026-83395	6.5 MEDIUM
CVE-2026-83400	5.3 MEDIUM
CVE-2026-87255	3.7 LOW
CVE-2026-87290	5.9 MEDIUM
CVE-2026-87291	5.3 MEDIUM
CVE-2026-87292	3.7 LOW
CVE-2026-87293	5.4 MEDIUM
CVE-2026-87294	6.5 MEDIUM
CVE-2026-87367	3.7 LOW
CVE-2026-91332	5.3 MEDIUM
CVE-2026-91333	3.7 LOW
CVE-2026-91334	3.7 LOW
CVE-2026-91335	2.6 LOW
CVE-2026-91373	5.3 MEDIUM
CVE-2026-91374	4.8 MEDIUM
CVE-2026-91375	4.7 MEDIUM
CVE-2026-91379	4.7 MEDIUM
CVE-2026-91380	4.0 MEDIUM
CVE-2026-91381	3.7 LOW
CVE-2026-91382	6.5 MEDIUM
CVE-2026-91385	5.4 MEDIUM
CVE-2026-91394	5.9 MEDIUM
CVE-2026-91395	6.5 MEDIUM
CVE-2026-91396	6.5 MEDIUM
CVE-2026-91397	3.6 LOW
CVE-2026-91398	6.8 MEDIUM

CVE	CVSS Score
CVE-2026-91400	3.1 LOW
CVE-2026-91402	3.1 LOW
CVE-2026-91409	3.7 LOW
CVE-2026-91410	5.3 MEDIUM
CVE-2026-91411	6.5 MEDIUM
CVE-2026-91415	7.0 HIGH
CVE-2026-91417	5.3 MEDIUM
CVE-2026-91418	5.3 MEDIUM
CVE-2026-91451	5.3 MEDIUM
CVE-2026-91452	5.3 MEDIUM
CVE-2026-91453	5.3 MEDIUM
CVE-2026-91461	3.7 LOW
CVE-2026-91462	5.9 MEDIUM
CVE-2026-91463	5.3 MEDIUM
CVE-2026-91464	5.3 MEDIUM
CVE-2026-91477	3.1 LOW
CVE-2026-91484	7.5 HIGH
CVE-2026-91487	4.8 MEDIUM
CVE-2026-101516	6.5 MEDIUM
CVE-2026-101737	5.9 MEDIUM

CWE's

CWE	Beschrijving
CWE-369	Divide By Zero
CWE-416	Use After Free
CWE-843	Access of Resource Using Incompatible Type ("Type Confusion")
CWE-863	Incorrect Authorization

Getroffen producten

Oracle
GraalVM
Java Se
JavaFX
Oracle GraalVM Enterprise Edition
Oracle GraalVM for JDK
Oracle Java SE
Oracle JavaFX

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 or 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.