



NCSC-2024-0419

Kwetsbaarheden verholpen in Oracle Java

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 17-10-2024

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 Java SE en GraalVM.

Duiding

Een kwaadwillende kan de kwetsbaarheden misbruiken om aanvallen uit te voeren die kunnen leiden tot de volgende categorieën schade:

- Denial-of-Service (DoS)
- Manipuleren van data
- Uitvoer van willekeurige code (Gebruikersrechten)
- Toegang tot gevoelige gegevens

Voor succesvol misbruik moet de kwaadwillende het slachtoffer misleiden om onvertrouwde code te importeren en uitvoeren. Deze kwetsbaarheden vormen daarom met name een risico voor ontwikkelaars en (lokale) gebruikers met rechten om code te importeren en uitvoeren.

Oplossingen

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

Referenties

➤ <https://www.oracle.com/security-alerts/cpuoct2024.html>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2023-7104	7.3 HIGH
➤ CVE-2023-42950	8.8 HIGH
➤ CVE-2024-21208	3.7 LOW
➤ CVE-2024-21210	3.7 LOW
➤ CVE-2024-21211	3.7 LOW

> CVE-2024-21217	3.7 LOW
> CVE-2024-21235	4.8 MEDIUM
> CVE-2024-25062	7.5 HIGH
> CVE-2024-36138	

CWE's

CWE	Beschrijving
> CVE-130	Improper Handling of Length Parameter Inconsistency
> CVE-195	Signed to Unsigned Conversion Error
> CVE-77	Improper Neutralization of Special Elements used in a Command ('Command Injection')
> CVE-190	Integer Overflow or Wraparound
> CVE-416	Use After Free
> CVE-122	Heap-based Buffer Overflow
> CVE-789	Memory Allocation with Excessive Size Value

Getroffen producten

oracle_corporation
graalvm
oracle_java_se
oracle
graalvm_for_jdk
graalvm
database_server
java_se

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.