Nationaal Cyber Security Centrum
*Ministerie van Justitie en Veiligheid*

# NCSC-2026-0314

## Kwetsbaarheden verholpen in Oracle Java SE

NCSC Security Advisory
Prioriteit: Normaal
Gepubliceerd op: 19-08-2026

**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, Oracle GraalVM for JDK en Oracle GraalVM Enterprise Edition.

## Duiding

De kwetsbaarheden betreffen meerdere ondersteunde versies van Oracle Java SE, Oracle GraalVM for JDK en Oracle GraalVM Enterprise Edition. Een onbevoegde aanvaller met netwerktoegang kan via verschillende aanvalsvectoren ongeautoriseerde toegang verkrijgen tot bepaalde of alle beschikbare data, waarbij sommige kwetsbaarheden leiden tot volledige compromittering van het systeem inclusief privilege-escalatie en uitvoering van ongeautoriseerde acties. Daarnaast zijn er kwetsbaarheden die een denial of service veroorzaken door het laten crashen of vastlopen van systemen, onder andere via sandboxed Java Web Start-applicaties en applets. Sommige kwetsbaarheden zijn te misbruiken via HTTP of TLS zonder authenticatie. De impact varieert van ongeautoriseerde gegevensonthulling tot verstoring van de beschikbaarheid van de Java runtime-omgevingen.

## Oplossingen

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

## Referenties

- https://www.oracle.com/security-alerts/cspuaug2026.html

## Kwetsbaarheden

| CVE | CVSS Score |
|---|---|
| CVE-2026-60589 | 3.7 LOW |
| CVE-2026-61308 | 6.8 MEDIUM |
| CVE-2026-62574 | 7.8 HIGH |
| CVE-2026-70906 | 7.5 HIGH |
| CVE-2026-70907 | 5.3 MEDIUM |

## CWE's

| CWE | Beschrijving |
|---|---|
| CWE-284 | Improper Access Control |

## Getroffen producten

| **Oracle** |
|---|
| Oracle GraalVM Enterprise Edition |
| Oracle GraalVM for JDK |
| Oracle Java SE |

## Disclaimer