Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0380

Kwetsbaarheden verholpen in Oracle Java SE

NCSC Security Advisory
Prioriteit: Normaal
Gepubliceerd op: 16-09-2026

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 3 kwetsbaarheden verholpen in Oracle Java SE, waaronder Oracle GraalVM for JDK en Oracle GraalVM Enterprise Edition.

Duiding

De kwetsbaarheden betreffen verschillende beveiligingsproblemen in Oracle Java SE-producten, waarbij niet-geauthenticeerde kwaadwillenden via netwerktoegang kwetsbaarheden in de Compiler-component kunnen misbruiken. De kwetsbaarheden hebben CVSS-scores in de categorie hoog. Alle drie de kwetsbaarheden kunnen volgens Oracle zonder authenticatie op afstand worden misbruikt. Succesvol misbruik kan onder meer leiden tot het verkrijgen van ongeautoriseerde toegang tot gevoelige informatie, het wijzigen van gegevens en het verstoren van de beschikbaarheid van getroffen systemen.

Geen van de kwetsbaarheden is als kritiek aangemerkt. CVE-2026-83357 en CVE-2026-83408 hebben met een CVSS-score van 8,1 de hoogste score en bevinden zich in de Compiler-component van Oracle GraalVM for JDK. Voor beide kwetsbaarheden is geen authenticatie of gebruikersinteractie vereist. Oracle geeft aan dat de kwetsbaarheden moeilijk te misbruiken zijn, maar dat succesvolle exploitatie kan leiden tot volledige overname van het getroffen product.

Oplossingen

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

Referenties

- https://www.oracle.com/security-alerts/cspusep2026.html

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-83357	8.1 HIGH
CVE-2026-83368	7.0 HIGH
CVE-2026-83408	8.1 HIGH

CWE's

CWE	Beschrijving
CWE-787	Out-of-bounds Write

Getroffen producten

Oracle
GraalVM
Oracle GraalVM Enterprise Edition
Oracle Corporation
Oracle GraalVM for JDK, Oracle GraalVM

Disclaimer