Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0261

Kwetsbaarheden verholpen in Oracle Java SE

NCSC Security Advisory
Prioriteit: Normaal
Gepubliceerd op: 22-07-2026

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 meerdere kwetsbaarheden verholpen in Java SE (inclusief Oracle GraalVM en JavaFX componenten).

Duiding

Oracle Java SE en gerelateerde producten (Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition) bevatten diverse kwetsbaarheden die een niet-geauthenticeerde aanvaller met netwerktoegang via TLS of andere API's in staat stellen om gedeeltelijke denial of service te veroorzaken, kritieke data te wijzigen, of ongeautoriseerde lees- en schrijfacties uit te voeren. Deze kwetsbaarheden treffen meerdere ondersteunde versies en componenten, waaronder JSSE, JavaFX, 2D component APIs, scripting componenten en sandboxed Java Web Start applicaties of applets. Sommige kwetsbaarheden vereisen gebruikersinteractie en/of lage privileges, terwijl andere ook zonder aanwezigheid van onbetrouwbare Java Web Start applicaties kunnen worden misbruikt. De impact varieert van denial of service tot ongeautoriseerde datawijziging en systeemcompromittering. Verschillende CVSS-scores zijn toegekend, variërend van laag (3.1) tot hoger (7.8), afhankelijk van de specifieke kwetsbaarheid en exploitatiemogelijkheden.

Oplossingen

Oracle heeft updates uitgebracht om de kwetsbaarheden in Java SE (inclusief Oracle GraalVM en JavaFX componenten) te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://www.oracle.com/security-alerts/cpujul2026.html
- https://www.oracle.com/security-alerts/cpujul2026verbose.html

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-41254	2.0 LOW
CVE-2026-46917	5.3 MEDIUM
CVE-2026-46968	5.9 MEDIUM
CVE-2026-47010	3.7 LOW
CVE-2026-47013	5.3 MEDIUM

CVE-2026-47021	5.3 MEDIUM
CVE-2026-47027	5.3 MEDIUM
CVE-2026-47030	5.3 MEDIUM
CVE-2026-47034	3.1 LOW
CVE-2026-47035	3.1 LOW
CVE-2026-47057	7.5 HIGH
CVE-2026-47058	7.4 HIGH
CVE-2026-47059	3.7 LOW
CVE-2026-47063	7.5 HIGH
CVE-2026-60147	6.5 MEDIUM
CVE-2026-60164	3.1 LOW
CVE-2026-60166	3.1 LOW
CVE-2026-60526	6.7 MEDIUM
CVE-2026-62574	7.8 HIGH

CWE's

CWE	Beschrijving
CWE-190	Integer Overflow or Wraparound
CWE-265	Privilege Issues
CWE-295	Improper Certificate Validation
CWE-347	Improper Verification of Cryptographic Signature
CWE-400	Uncontrolled Resource Consumption
CWE-476	NULL Pointer Dereference
CWE-696	Incorrect Behavior Order

CWE-787	Out-of-bounds Write
CWE-1333	Inefficient Regular Expression Complexity

Getroffen producten

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

Disclaimer