Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0383

Kwetsbaarheden verholpen in Oracle VM VirtualBox

NCSC Security Advisory
Prioriteit: Normaal
Gepubliceerd op: 17-09-2026

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 19 kwetsbaarheden verholpen in Oracle VM VirtualBox.

Duiding

De kwetsbaarheden betreffen verschillende beveiligingsproblemen in Oracle VM VirtualBox, waaronder mogelijkheden voor lokale en geauthenticeerde kwaadwillenden om ongeautoriseerde acties uit te voeren. De kwetsbaarheden hebben CVSS-scores variërend van laag tot hoog. Van de in totaal 19 kwetsbaarheden kan volgens Oracle één kwetsbaarheid 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. Voor het merendeel van de kwetsbaarheden is lokale toegang, gebruikersinteractie of voorafgaande toegangsrechten vereist.

Geen van de kwetsbaarheden is als kritiek aangemerkt. CVE-2026-87273 heeft met een CVSS-score van 8,6 de hoogste score en kan lokaal worden misbruikt waarbij gebruikersinteractie vereist is. Succesvolle exploitatie kan een hoge impact hebben op de vertrouwelijkheid, integriteit en beschikbaarheid van het getroffen systeem. CVE-2026-87277 heeft een CVSS-score van 7,5 en kan zonder authenticatie op afstand via RDP worden misbruikt. Succesvolle exploitatie kan leiden tot verstoring van de beschikbaarheid van het getroffen systeem.

Oplossingen

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

Referenties

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

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-87267	5.3 MEDIUM
CVE-2026-87268	7.8 HIGH
CVE-2026-87269	7.8 HIGH
CVE-2026-87270	7.8 HIGH

CVE-2026-87271	7.8 HIGH
CVE-2026-87272	7.8 HIGH
CVE-2026-87273	8.6 HIGH
CVE-2026-87274	4.4 MEDIUM
CVE-2026-87275	4.6 MEDIUM
CVE-2026-87276	7.5 HIGH
CVE-2026-87277	7.5 HIGH
CVE-2026-87278	6.1 MEDIUM
CVE-2026-87279	6.1 MEDIUM
CVE-2026-87280	4.2 MEDIUM
CVE-2026-87281	3.2 LOW
CVE-2026-87282	6.0 MEDIUM
CVE-2026-87283	6.0 MEDIUM
CVE-2026-87284	3.2 LOW
CVE-2026-87285	6.0 MEDIUM

CWE's

CWE	Beschrijving
CWE-764	Multiple Locks of a Critical Resource
CWE-862	Missing Authorization

Getroffen producten

Oracle
Oracle VM VirtualBox
VM

Disclaimer