Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0269

Kwetsbaarheden verholpen in VMware producten

NCSC Security Advisory
Prioriteit: Normaal
Gepubliceerd op: 29-07-2026

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

VMware heeft kwetsbaarheden verholpen in VMware vCenter en VMware ESX producten.

Duiding

VMware vCenter bevat een kritieke authentication-bypass kwetsbaarheid in de Directory Service met kenmerk CVE-2026-59309. Deze kwetsbaarheid stelt een kwaadwillende met netwerktoegang tot VMware vCenter in staat deze kwetsbaarheid te misbruiken om de authenticatie te omzeilen en ongeautoriseerde toegang tot het systeem te verkrijgen.

Daarnaast bevat VMware vCenter ook een kritieke directory-traversal kwetsbaarheid in de Syslog server met kenmerk CVE-2026-59310. Deze kwetsbaarheid kan een kwaadwillende in staat stellen willekeurige code uit te voeren, waardoor mogelijk bestands- en directorypaden kunnen worden gemanipuleerd en toegang kan worden verkregen tot bestanden buiten de bedoelde Syslog-directory.

VMware ESXi bevat een kritieke out-of-bounds write kwetsbaarheid in de VMXNET3 virtuele netwerkadapter met kenmerk CVE-2026-47876. Deze kwetsbaarheid stelt een kwaadwillende met lokale beheerdersrechten op een virtuele machine met een VMXNET3 virtuele netwerkadapter in staat, code uit te voeren op de onderliggende host. Dit maakt het voor een kwaadwillende mogelijk, data buiten de bedoelde geheugenlimieten kan schrijven, wat kan leiden tot geheugenbeschadiging en onvoorspelbaar gedrag of compromittering van het virtuele systeem. Virtuele netwerkadapters die geen gebruikmaken van VMXNET3 zijn niet kwetsbaar.

In VMware ESX, Workstation en Fusion bevatten ook een out-of-bounds read kwetsbaarheid met kenmerk CVE-2026-41703. Misbruik van deze kwetsbaarheid die kan resulteren in onbedoelde toegang tot geheugen buiten de toegewezen buffer, wat kan leiden tot informatielekken of systeeminstabiliteit binnen virtuele omgevingen. Daarnaast bevat VMware ESX een kwetsbaarheid met kenmerk CVE-2026-41709 door onvoldoende logging. Een kwaadwillende beheerder kan deze kwetsbaarheid misbruiken om bepaalde acties uit te voeren die niet in de logbestanden worden geregistreerd.

Het is goed gebruik om toegang tot ESXi en vCenter uitsluitend beschikbaar te stellen vanuit een gescheiden beheeromgeving waarin alleen geautoriseerde beheerders toegang hebben. Deze beheerinterfaces dienen niet rechtstreeks vanaf internet of externe netwerken toegankelijk te zijn.

Oplossingen

VMware heeft updates uitgebracht om de kwetsbaarheden in VMware vCenter, ESX, Workstation en Fusion te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://brcm.tech/vmsa-2026-0006
- https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/38017

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-59309	9.8 CRITICAL
CVE-2026-59310	9.8 CRITICAL
CVE-2026-47876	9.3 CRITICAL
CVE-2026-41703	7.6 HIGH
CVE-2026-41709	2.7 LOW

CWE's

CWE	Beschrijving
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
CWE-125	Out-of-bounds Read
CWE-778	Insufficient Logging

Getroffen producten

VMware
ESX
Fusion
Workstation
vCenter

Disclaimer