Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0073

Kwetsbaarheden verholpen in VMware producten

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 04-03-2025

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

Broadcom heeft kwetsbaarheden verholpen in VMware ESXi (inclusief Workstation en Fusion).

Duiding

De kwetsbaarheden omvatten een TOCTOU-kwetsbaarheid die een kwaadwillende met lokale administratieve rechten in staat stelt om code uit te voeren als het VMX-proces op de host via een out-of-bounds write. Daarnaast is er een arbitrarily write-kwetsbaarheid die het mogelijk maakt voor een kwaadwillende met privileges in het VMX-proces om kernel writes uit te voeren, wat kan leiden tot ontsnapping uit de sandbox-omgeving. Ook is er een informatielek-kwetsbaarheid door een out-of-bounds read in HGFS, wat kan leiden tot geheugenlekken vanuit het VMX-proces.

Van de kwetsbaarheid met kenmerk CVE-2025-22226 meldt Broadcom informatie te hebben dat deze actief is misbruikt.

Oplossingen

Broadcom heeft patches uitgebracht om de kwetsbaarheden te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

› https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25390

Kwetsbaarheden

CVE	CVSS Score
› CVE-2025-22224	9.3 CRITICAL
› CVE-2025-22225	8.2 HIGH
› CVE-2025-22226	7.1 HIGH

CWE's

CWE	Beschrijving
CWE-125	Out-of-bounds Read
CWE-787	Out-of-bounds Write

Getroffen producten

VMWare
Workstation
VMware
Cloud Foundation
ESXi
Fusion
Telco Cloud Infrastructure
Telco Cloud Platform

Disclaimer