Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0171

Kwetsbaarheden verholpen in VMware producten

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 21-05-2025

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) en vCenter Server.

Duiding

De kwetsbaarheden omvatten een command-executie kwetsbaarheid in vCenter Server, die geauthenticeerde aanvallers in staat stelt om willekeurige code op de server uit te voeren. Verder is er een denial-of-service kwetsbaarheid in VMware ESXi die kan worden geëxploiteerd door niet-administratieve gebruikers binnen een gastbesturingssysteem, wat kan leiden tot uitputting van het geheugen van het hostproces. Tot slot is er een gereflecteerde cross-site scripting kwetsbaarheid in VMware ESXi en vCenter Server, die voortkomt uit onjuiste invoervalidatie, waardoor kwaadwillenden mogelijk cookies kunnen stelen of gebruikers kunnen omleiden naar schadelijke websites.

Oplossingen

Broadcom heeft updates 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/0/25717

Kwetsbaarheden

CVE	CVSS Score
› CVE-2025-41225	8.8 HIGH
› CVE-2025-41226	6.8 MEDIUM
› CVE-2025-41227	5.5 MEDIUM
› CVE-2025-41228	4.3 MEDIUM

CWE's

CWE	Beschrijving
CWE-400	Uncontrolled Resource Consumption
CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Getroffen producten

VMware
vCenter Server
Cloud Foundation
VMware Cloud Foundation (ESXi)
VMware Telco Cloud Platform (vCenter)
VMware Workstation
VMware Fusion

Disclaimer