



# 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](http://www.first.org/tlp)).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op [info@ncsc.nl](mailto: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
➤ <a href="#">CVE-2025-41225</a>	8.8 HIGH
➤ <a href="#">CVE-2025-41226</a>	6.8 MEDIUM
➤ <a href="#">CVE-2025-41227</a>	5.5 MEDIUM
➤ <a href="#">CVE-2025-41228</a>	4.3 MEDIUM

## CWE's

CWE	Beschrijving
> <a href="#">CWE-400</a>	Uncontrolled Resource Consumption
> <a href="#">CWE-78</a>	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
> <a href="#">CWE-79</a>	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

The Netherlands Cyber Security Center (henceforth: NCSC-NL) maintains this page to enhance access to its information and security advisories. The use of this security advisory is subject to the following terms and conditions: NCSC-NL makes every reasonable effort to ensure that the content of this page is kept up to date, and that it is accurate and complete. Nevertheless, NCSC-NL cannot entirely rule out the possibility of errors, and therefore cannot give any warranty in respect of its completeness, accuracy or continuous keeping up-to-date. The information contained in this security advisory is intended solely for the purpose of providing general information to professional users. No rights can be derived from the information provided therein. NCSC-NL and the Kingdom of the Netherlands assume no legal liability or responsibility for any damage resulting from either the use or inability of use of this security advisory. This includes damage resulting from the inaccuracy of incompleteness of the information contained in the advisory. This security advisory is subject to Dutch law. All disputes related to or arising from the use of this advisory will be submitted to the competent court in The Hague. This choice of means also applies to the court in summary proceedings.