



# 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](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).

## 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
➤ <a href="#">CVE-2025-22224</a>	9.3 CRITICAL
➤ <a href="#">CVE-2025-22225</a>	8.2 HIGH
➤ <a href="#">CVE-2025-22226</a>	7.1 HIGH

## CWE's

CWE	Beschrijving
<a href="#">&gt; CWE-125</a>	Out-of-bounds Read
<a href="#">&gt; CWE-787</a>	Out-of-bounds Write

## Getroffen producten

<b>VMWare</b>
Workstation
<b>VMware</b>
Cloud Foundation
ESXi
Fusion
Telco Cloud Infrastructure
Telco Cloud Platform

## 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.