VMware ESXi – VMSA-2025-0004

Overview

On March 4, 2025, Broadcom published a security advisory detailing three vulnerabilities impacting VMware ESXi. These vulnerabilities include time-of-check/time-of-use, arbitrary write, and information disclosure. This advisory references Broadcom's security advisory article, VMSA-2025-0004.

Affected Products and Versions

VMware ESXi – All Versions

- Control Server
- Baseline Security Center (BSC)
- OTarmor
- Monitoring & Diagnostics On-Site Monitor (OSM)

Vulnerability Details

ISSUE	BASE SCORE	ADJUSTED SCORE	PLATFORM	DESCRIPTION
CVE-2025-22224	9.3 (Critical)	7.4 (High)	ESXi	TOCTOU Race Condition (CWE-367)
CVE-2025-22225	8.2 (High)	7.4 (High)	ESXi	Out of Bounds Write (CWE-787)
CVE-2025-22226	7.1 (High)	3.0 (Low)	ESXi	Out of Bounds Read (CWE-125)

Note: Adjusted Score is an environmental score calculated according to impact with regards to compensating controls and overall system impact in the customer environment.

Exploitation Status

GE Vernova has not observed or received any reports of compromised Gas Power customer equipment due to this vulnerability. However, Broadcom has reported that all three vulnerabilities have been exploited in the wild.

Remediation/Mitigation

GE Vernova has validated the following patches for installation on Control Server installations, additionally covering BSC and OTarmor installations:

ESXi 8.0 U3d-24585383
ESXi 8.0 U2d-24585300
ESXi 7.0 U3s-24585291

Additionally, while Broadcom has released a patch for ESXi 6.7, GE Vernova has not validated this update as 6.7 is past Broadcom's end of general support date. GE Vernova recommends that customers using ESXi version 6.7 or earlier upgrade to one of the versions listed above. Please contact your local GE Vernova Services representative for support.

For M&D customers, ESXi 7.0 U3s is being deployed to fleet OSMs, and no action is required on your part.

Additional Information

To determine the current version of ESXi installed, you can use either of the two below methods provided by Broadcom.

Using the vSphere Client:

1. Using the vSphere Client log in to ESX/ESXi host.
2. In the **Hosts and Clusters** view, click the **ESX/ESXi host** in the inventory.
3. Above the tabs, look to the line that identifies the host. This line includes the build number of the selected ESX/ESXi host.

Using the ESXi Console:

1. Log in to the ESX/ESXi host at the console as root.
2. Press Alt + F1 to ESXi Shell.
3. Type **vmware -v** and press Enter.

Contact Information

Contact your local GE Vernova Services representative for assistance or additional information.
For Product Security issues or incident/vulnerability reporting: https://www.gevernova.com/security

Document History

Version	Release Date	Purpose
1.0	4/15/2025	Initial Release

Disclaimer

Unless the product is under a GE Vernova service contract, GE Vernova assumes no responsibility or liability for the content of Security Notices or for making Security Notices available to customer. Implementing Security Notices as well as performing updates/upgrades to software/firmware is solely the responsibility of the customer.