

VMware ESXi and vCenter: VMSA-2026-0006

Overview

On July 29, 2026, Broadcom published [VMSA-2026-0006](#) detailing multiple vulnerabilities impacting VMware ESXi and vCenter.

Affected Products and Versions

Control Server

BSC

OTArmor*

GE Vernova Digital Servers

ESXi < 8.0 U3k

vCenter < 8.0 U3k

Vulnerability Details

ISSUE	BASE SCORE	ADJUSTED SCORE	PLATFORM	DESCRIPTION
CVE-2026-59309	9.8 (Critical)	7.2 (High)	vCenter	Incorrect implementation of authentication (CWE-303)
CVE-2026-59310	9.8 (Critical)	7.2 (High)	vCenter	Path traversal (CWE-22)
CVE-2026-47876	9.3 (Critical)	8.1 (High)	ESXi	Out of bounds write (CWE-787)
CVE-2026-41703	7.6 (High)	4.4 (Medium)	ESXi	Out of bounds read (CWE-125)
CVE-2026-41709	2.7 (Low)	2.0 (Low)	ESXi	Insufficient logging (CWE-778)

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

CVE-2026-59309: vCenter authentication bypass

CVE-2026-59310: vCenter directory traversal

CVE-2026-47876: VMXNET3 out of bounds write

CVE-2026-41703: Out of bounds read

CVE-2026-41709: ESX insufficient logging

Exploitation Status

GE Vernova has not yet observed or received any reports that Gas Power customer equipment has been compromised due to this vulnerability.

Remediation/Mitigation (Gas Power Customers)

Gas Power Controls has validated ESXi and vCenter Server updates 8.0 U3k. Update steps for both platforms are provided below.

Update Process for vCenter Server Appliance:

- 1.) Ensure there is a backup of the VCSA server
- 2.) Copy the patch-FP.iso file to the local datastore on the host that has VCSA
- 3.) Edit the VCSA settings > CD > Datastore ISO > find the update ISO file uploaded in the

© 2025 GE Vernova. All rights reserved. GE Vernova reserves the right to vary its findings and conclusions should any information or technical knowledge come to GE Vernova after the date of this document. This Security Advisory does not vary any contractual relationship between GE Vernova and its customer. NO REPRESENTATION OR WARRANTY IS MADE OR IMPLIED AS TO ITS COMPLETENESS, ACCURACY, OR FITNESS FOR ANY PARTICULAR PURPOSE.

*Trademark of GE Vernova and/or its affiliates

previous step, ensure the "connect" check box is checked

4.) Log in to the VCSA VAMI as the root user "https://vcsa.hmi.local:5480". The FQDN may be different but the port 5480 is the same on all VCSA servers.

5.) Click the Update Tab on the left menu

6.) Click Check Updates and select "Check CD ROM"

7.) Review the update and click Stage and Install, then accept the EULA

8.) Confirm you have a backup of the system on the next screen and click Finish to begin the installation

Update Process for ESXi Hosts:

NOTE: This patch requires the ESXi host to be put into Maintenance mode and all VMs either migrated to other hosts in the cluster or shut down. A reboot is required after patch installation is completed.

1.) Download from the Broadcom portal (VMware-ESXi-8.0U3k-25595708-depot.zip)

2.) Create a folder on the boot controller datastore called "update"

3.) Upload the zip file to the datastore folder you just created on the ESXi host using the vSphere client web UI (datastore browser)

4.) Enable SSH and ESXi Shell services on the ESXi host (TSM - Tech Support Mode)

5.) Migrate VMs to another host in the cluster or power down the VMs, then place the ESXi host into maintenance mode.

6.) Use Putty to connect to the ESXi host via SSH and log in as the root user

7.) issue the following command to install the update:

```
esxcli software profile update -p ESXi-8.0U3k-25595708-standard -d /vmfs/volumes/685c9717-4348be00-a912-8cdcd40b57f0/update/VMware-ESXi-8.0U3g-24859861-depot.zip
```

Note: In the command above the FULL path to the datastore will be different on every ESXi host. in the example above the long string of 685c9717... will be unique. Additionally, viewing the ESXi VMs via vCenter after updating may show a warning that VMware Tools requires an update – this update is part of the ESXi package and the Tools update can be applied safely to these VMs.

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	09/03/2026	Initial Release

Disclaimer

GE Vernova assumes no responsibility or liability for the content of Security Notices or for making Security Notices available to customer. Any rights and remedies arising out of or in connection with this Security Notice are subject to the applicable terms of a GE Vernova contract.