VMware vCenter Server – VMSA-2024-0019 Heap Overflow and Privilege Escalation Vulnerabilities

Overview

A pair of vulnerabilities were disclosed by Broadcom on September 17th, 2024, detailing a heap overflow (CVE-2024-38812) and privilege escalation (CVE-2024-38813) vulnerability. This advisory references Broadcom's VMSA-2024-0019 security advisory.

Important Update – November 18th, 2024

On November 18th, 2024, Broadcom updated the original advisory to communicate that these vulnerabilities are not fully addressed by applying the 8.0 U3b or 7.0 U3s patches as previously stated. GE Vernova has not yet completed validation of the new 8.0 U3d or 7.0 U3t patches for existing sites and will update this advisory once validation is complete.

Affected Products and Versions

VMware vCenter Server 8.0 U3a and below
VMware vCenter Server 7.0 U3r and below

Vulnerability Details

ISSUE	BASE SCORE	ADJUSTED SCORE	PLATFORM	DESCRIPTION
CVE-2024-38812	9.8 (Critical)	8.1 (High)	vCenter Server	Heap-Based Buffer Overflow (CWE-122)
CVE-2024-38813	7.5 (High)	6.7 (Medium)	vCenter Server	Improper Check for Dropped Privileges (CWE-273)

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

For Gas Power customers, these vulnerabilities impact Control Server installations utilizing VMware vCenter Server.

Exploitation Status

GE Vernova has not yet observed nor received reports of any compromise of Gas Power customer equipment due to these vulnerabilities.

Remediation/Mitigation

GE Vernova has completed validation for both vCenter Server 8.0 U3b and 7.0 U3s and recommends updating your local installation to the appropriate patch matching your major version. You can check your vCenter Server version by utilizing the vSphere Client to log in to the vCenter Server, then navigating to Help -> About VMware vSphere.

Please note that vCenter Server 8.0 U3b has a known issue which can cause a number of issues after installation; for customers updating to this version, there is a workaround detailed in the KB377734 knowledge article provided by Broadcom.

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
2.0	11/27/2024	Original fix replaced and requires validation
1.0	10/7/2024	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.