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

Overview

A pair of vulnerabilities were disclosed by Broadcom on September 17, 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.

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 that use VMware vCenter Server.

Exploitation Status

GE Vernova has not yet observed nor received reports of any Gas Power customer equipment being compromised by 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 into 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
1.0	10/28/2024	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.