VMware vCenter Server and vSphere ESXi Multiple Vulnerabilities

Overview

Several VMware vulnerabilities impacting ESXi and vCenter were published on May 21st, 2024 and June 18th, 2024, under the IDs CVE-2024-22273, CVE-2024-22274, CVE-2024-22275, CVE-2024-37079, CVE-2024-37080, and CVE-2024-37081. These vulnerabilities impact GE Vernova's ControlST platform, which utilizes both vCenter Server and vSphere ESXi.

Affected Products and Versions

ControlST – Control Server

Vulnerability Details

CVE ID	BASE SCORE	ADJUSTED SCORE	PLATFORM	DESCRIPTION
CVE-2024-22273	8.1 (High)	6.3 (Medium)	vSphere ESXi	Out-of-bounds read/write
CVE-2024-22274	7.2 (High)	6.7 (Medium)	vCenter Server	Authenticated remote-code execution
CVE-2024-22275	4.9 (Medium)	4.4 (Medium)	vCenter Server	Partial file read
CVE-2024-37079	9.8 (Critical)	8.4 (High)	vCenter Server	Heap overflow
CVE-2024-37080	9.8 (Critical)	8.4 (High)	vCenter Server	Heap overflow
CVE-2024-37081	7.8 (High)	7.0 (High)	vCenter Server	Local privilege escalation

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 yet observed nor received reports of any compromise of Gas Power customer equipment due to these vulnerabilities.

Remediation/Mitigation

A patch should be applied to the vCenter Server on the Control Server device; both vCenter 7.0U3r and 8.0U2d have been validated by GE Vernova and are approved for installation at customer sites. Please contact your local GE Vernova Services representative for instructions and support with applying either of these patches, as some additional configuration may be required to ensure correct operation.
The ESXi installation does not need to be modified at this time.

Contact Information

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

Document History

Version	Release Date	Purpose
1.0	9/18/2024	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.