VMware warns of critical vulnerability affecting vCenter Server product

2023-10-30 - Arnis Morkāns - Comments (0) - General

Advisory ID:VMSA-2023-0023

CVSSv3 Range:4.3-9.8

Issue Date:2023-10-25

Updated On:2023-10-25 (Initial Advisory)

CVE(s):CVE-2023-34048, CVE-2023-34056

Synopsis:VMware vCenter Server updates address out-of-bounds write and information disclosure vulnerabilities (CVE-2023-34048, CVE-2023-34056)

Impacted Products

- VMware vCenter Server
- VMware Cloud Foundation

2. Introduction

An out-of-bounds write (CVE-2023-34048) and a partial information disclosure (CVE-2023-34056) in vCenter Server were responsibly reported to VMware. Updates are available to remediate these vulnerabilities in affected VMware products.

3a. VMware vCenter Server Out-of-Bounds Write Vulnerability (CVE-2023-34048)

Description

vCenter Server contains an out-of-bounds write vulnerability in the implementation of the DCERPC protocol. VMware has evaluated the severity of this issue to be in the Critical severity range with a maximum CVSSv3 base score of 9.8.

Known Attack Vectors

A malicious actor with network access to vCenter Server may trigger an out-of-bounds write potentially leading to remote code execution.

Resolution

To remediate CVE-2023-34048 apply the updates listed in the 'Fixed Version' column of the 'Response Matrix' below to affected deployments.

Workarounds

In-product workarounds were investigated, but were determined to not be viable.

Additional Documentation

A supplemental FAQ was created for additional clarification. Please see: https://via.vmw.com/vmsa-2023-0023-qna

Notes

- While VMware does not mention end-of-life products in VMware Security Advisories, due to the critical severity of this vulnerability and lack of workaround VMware has made a patch generally available for vCenter Server 6.7U3, 6.5U3, and VCF 3.x. For the same reasons, VMware has made additional patches available for vCenter Server 8.0U1.
- Async vCenter Server patches for VCF 5.x and 4.x deployments have been made available. Please see KB88287 for more information.

Acknowledgements

VMware would like to thank Grigory Dorodnov of Trend Micro Zero Day Initiative for reporting this issue to us.

3b. VMware vCenter Server Partial Information Disclosure Vulnerability (CVE-2023-34056)

Description

vCenter Server contains a partial information disclosure vulnerability. VMware has evaluated the severity of this issue to be in the Moderate severity range with a maximum CVSSv3 base score of 4.3.

Known Attack Vectors

A malicious actor with non-administrative privileges to vCenter Server may leverage this issue to access unauthorized data.

Resolution

To remediate CVE-2023-34056 apply the updates listed in the 'Fixed Version' column of the 'Response Matrix' below to affected deployments.

Workarounds

None.

Additional Documentation

None.

Acknowledgements

VMware would like to thank Oleg Moshkov of Deiteriy Lab OÜ for reporting this issue to us.

Response Matrix

Product	Version	Running On	CVE Identifier	CVSSv3	Severity	Fixed Version	Workarounds	Additional Documentation
VMware vCenter Server	8.0	Any	CVE-2023-34048, CVE-2023-34056	9.8, 4.3	Critical	8.0U2	None	FAQ
VMware vCenter Server	8.0	Any	CVE-2023-34048	9.8	Critical	8.0U1d	None	FAQ
VMware vCenter Server	7.0	Any	CVE-2023-34048, CVE-2023-34056	9.8, 4.3	Critical	7.0U3o	None	FAQ
VMware Cloud Foundation (VMware vCenter Server)	5.x, 4.x	Any	CVE-2023-34048, CVE-2023-34056	9.8, 4.3	Critical	KB88287	None	FAQ

4. References

Fixed Version(s) and Release Notes:

VMware vCenter Server 8.0U2
Downloads and Documentation:
https://customerconnect.vmware.com/downloads/details?downloadGroup=VC80U2&productId=1345&rPId=110105

VMware vCenter Server 8.0U1d
Downloads and Documentation:
https://customerconnect.vmware.com/downloads/details?downloadGroup=VC80U1D&productId=1345&rPId=112378

VMware vCenter Server 7.0U3o
Downloads and Documentation:
https://customerconnect.vmware.com/downloads/details?downloadGroup=VC70U3O&productId=974&rPId=110262

Cloud Foundation 5.x/4.x
https://kb.vmware.com/s/article/88287

Mitre CVE Dictionary Links
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-34048
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-34056

FIRST CVSSv3 Calculator
CVE-2023-34048: https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CVE-2023-34056: https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N

5. Change Log

2023-10-25 VMSA-2023-0023
Initial security advisory.

6. Contact

E-mail: security@vmware.com

PGP key at:
https://kb.vmware.com/kb/1055

VMware Security Advisories
https://www.vmware.com/security/advisories

VMware Security Response Policy
https://www.vmware.com/support/policies/security_response.html

VMware Lifecycle Support Phases
https://www.vmware.com/support/policies/lifecycle.html

VMware Security & Compliance Blog
https://blogs.vmware.com/security

Twitter
https://twitter.com/VMwareSRC

Copyright 2023 VMware Inc. All rights reserved.