



Threat Level

 **Amber**

HiveForce Labs

THREAT ADVISORY

 **VULNERABILITY REPORT**

VMware vCenter Flaws Leading to RCE Attacks

Date of Publication

October 27, 2023

Admiralty Code

A1

TA Number

TA2023437







Summary

First Discovered: October 25, 2023

Affected Product: VMware vCenter Server, VMware Cloud Foundation

Impact: Two vulnerabilities, CVE-2023-34048 and CVE-2023-34056, were identified in VMware vCenter Server, a server management software used for centralized management of virtual machines and ESXi hosts. CVE-2023-34048 is associated with an Out-of-Bounds Write issue, while CVE-2023-34056 is linked to Partial Information Disclosure. These vulnerabilities could allow an attacker to execute remote code and gain unauthorized access to sensitive information.

CVEs

CVE	NAME	AFFECTED PRODUCTS	ZERO-DAY	CISA	PATCH
CVE-2023-34048	VMware vCenter Out-of-Bounds Write Vulnerability	VMware vCenter Server, VMware Cloud Foundation			
CVE-2023-34056	VMware vCenter Information Disclosure Vulnerability	VMware vCenter Server, VMware Cloud Foundation			

Vulnerability Details

#1

VMware has address two vulnerabilities, CVE-2023-34048 an out-of-bounds write flaw and CVE-2023-34056 an information disclosure flaw affecting the vCenter Server. These vulnerabilities could allow an attacker to execute remote code and gain unauthorized access to sensitive information.

#2

The vulnerability CVE-2023-34048 is caused by a boundary error in the DCERPC protocol implementation. An attacker with network access can exploit this vulnerability by sending a specially crafted request to the vCenter Server leading to out-of-bounds write, potentially allowing remote code execution on the affected system.

#3

The vulnerability CVE-2023-34056 is a result of improper access restrictions. It allows a malicious actor with non-administrative privileges to bypass implemented security restrictions and gain access to unauthorized data on the vCenter Server. This could potentially lead to unauthorized access to sensitive information or data.

#4

VMware vCenter Server and related products users are strongly advised to upgrade to the latest versions to mitigate the risk of exploitation of the vulnerabilities CVE-2023-34048 and CVE-2023-34056. These fixes were released a month prior. It is essential to be cautious and ensure your system is patched to protect against potential attacks that might target these vulnerabilities.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-34048	vCenter Server: 7.0-7.0U3n 8.0- 8.0U1c, VMware Cloud Foundation 5.x, 4.x	cpe:2.3:a:vmware:vcenter-server:8.0:U1c:*:*:*:*:*	CWE-787
CVE-2023-34056	vCenter Server: 7.0-7.0U3n 8.0- 8.0U1c, VMware Cloud Foundation 5.x, 4.x	cpe:2.3:a:vmware:vcenter-server:8.0:U1d:*:*:*:*:*	CWE-284

Recommendations



Apply Patch: Install the security patch provided by VMware to address the CVE-2023-34048 and CVE-2023-34056 vulnerabilities. This patch closes the security gap that allows attackers to exploit the vulnerability.



Least Privilege: Adhere to the idea of "least privilege" by giving users only the essential permissions they need for their tasks. This strategy reduces the effects of vulnerabilities related to privilege escalation.



Implement Behavioral Analysis: Deploy advanced security solutions that employ behavioral analysis and monitoring on the host for detection of unusual activities and anomalies in the system. This proactive approach can help catch sophisticated threats before they fully compromise your systems.

Potential MITRE ATT&CK TTPs

<u>TA0042</u> Resource Development	<u>TA0001</u> Initial Access	<u>TA0002</u> Execution	<u>TA0004</u> Privilege Escalation
<u>T1588</u> Obtain Capabilities	<u>T1588.006</u> Vulnerabilities	<u>T1190</u> Exploit Public-Facing Application	

Patch Details

VMware has released updates for VMware vCenter Server and Cloud Foundation to address the vulnerabilities. Refer to the fixes below for specific versions.

VMware vCenter Server 8.0U2

<https://customerconnect.vmware.com/downloads/details?downloadGroup=VC80U2&productId=1345&rPId=110105>

VMware vCenter Server 8.0U1d (Only resolves CVE-2023-34048)

<https://customerconnect.vmware.com/downloads/details?downloadGroup=VC80U1D&productId=1345&rPId=112378>

VMware vCenter Server 7.0U3o

<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>

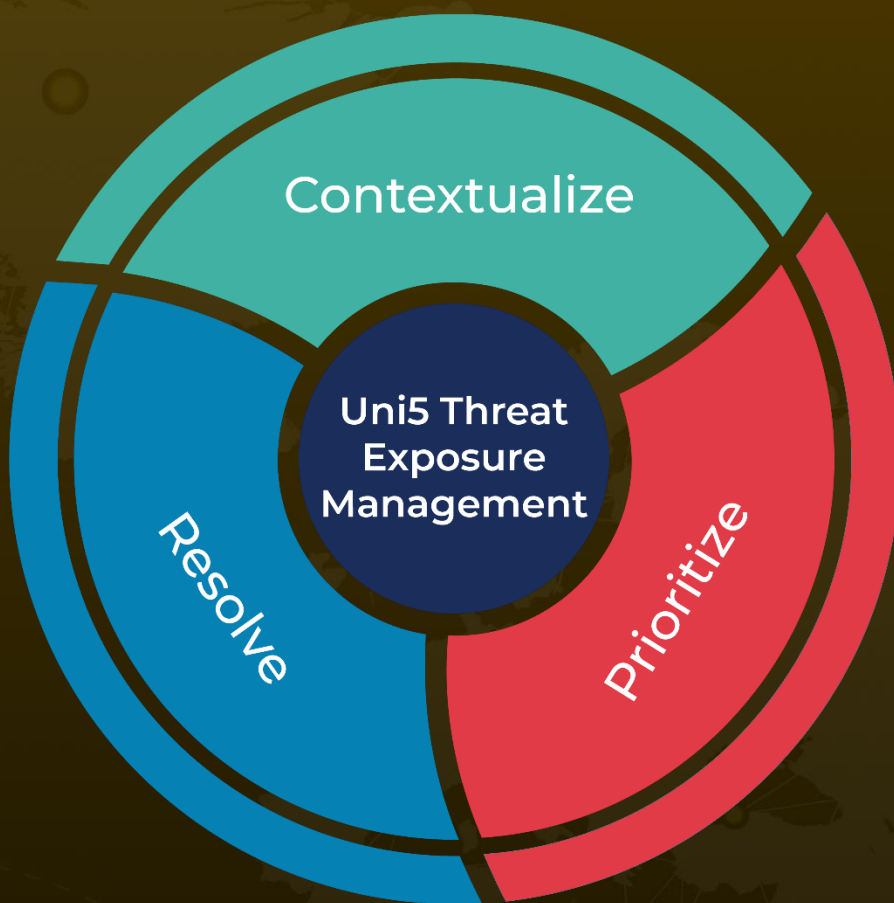
References

<https://www.vmware.com/security/advisories/VMSA-2023-0023.html>

What Next?

At Hive Pro, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with HivePro Uni5: Threat Exposure Management Platform.



REPORT GENERATED ON

October 27, 2023 • 5:20 AM

© 2023 All Rights are Reserved by Hive Pro®



More at www.hivepro.com