

HiveForce Labs

THREAT ADVISORY

 **VULNERABILITY REPORT**

VMware Address Critical Heap-Overflow and Privilege Escalation Flaws

Date of Publication

June 19, 2024

Admiralty Code

A1

TA Number

TA2024235

Summary

First Seen: June 2024

Affected Products: VMware vCenter Server, VMware Cloud Foundation

Impact: VMware addresses critical vulnerabilities in vCenter Server, including heap-overflow and privilege escalation flaws. The three identified vulnerabilities are CVE-2024-37079, CVE-2024-37080, and CVE-2024-37081. These vulnerabilities pose significant security risks, potentially allowing attackers to execute code remotely and escalate privileges locally, thereby compromising the affected systems.

⚙️ CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2024-37079	VMware vCenter Server Heap-overflow Vulnerability	VMware vCenter Server, VMware Cloud Foundation	✗	✗	✓
CVE-2024-37080	VMware vCenter Server Heap-overflow Vulnerability	VMware vCenter Server, VMware Cloud Foundation	✗	✗	✓
CVE-2024-37081	VMware vCenter Server Multiple Local Privilege Escalation Vulnerabilities	VMware vCenter Server, VMware Cloud Foundation	✗	✗	✓

Vulnerability Details

#1

VMware recently identified some serious issues affecting its Cloud Foundation and vCenter Server products. These vulnerabilities could allow attackers to do malicious stuff like taking over systems and gaining higher levels of access. These vulnerabilities affect VMware vCenter Server versions 7.0 and 8.0, as well as VMware Cloud Foundation versions 4.x and 5.x.

#2

CVE-2024-37079 and CVE-2024-37080 are both heap-overflow vulnerabilities. They happen because of errors in how a protocol called DCERPC is handled. Essentially, if an attacker sends specially crafted data to the system, it could cause a heap-based overflow. This lets them run their own code on the system. If successful, this could completely compromise the vulnerable system.

#3

CVE-2024-37081 is a privilege escalation flaw. It means a local user could exploit a misconfiguration in a system component called sudo to run code with higher privileges than they should have.

#4

Unfortunately, there are no quick fixes or built-in workarounds to protect against these issues. It's important to note that vulnerabilities like these are often targeted by cyber attackers once they become publicly known. Therefore, it is crucial for anyone using VMware's software to update their systems immediately. By doing so, you can help protect your data and systems from potential threats.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-37079	vCenter Server: 7.0 U1 - 8.0.0c Cloud Foundation versions 4.x and 5.x.	cpe:2.3:a:vmware:cloud_foundation:*:*:*:*:*:* cpe:2.3:a:vmware:vcenter_server:*:*:*:*:*:*	CWE-122
CVE-2024-37080	vCenter Server: 7.0 U1 - 8.0.0c Cloud Foundation versions 4.x and 5.x.	cpe:2.3:a:vmware:cloud_foundation:*:*:*:*:*:* cpe:2.3:a:vmware:vcenter_server:*:*:*:*:*:*	CWE-122
CVE-2024-37081	vCenter Server: 7.0 U1 - 8.0.0c Cloud Foundation versions 4.x and 5.x.	cpe:2.3:a:vmware:cloud_foundation:*:*:*:*:*:* cpe:2.3:a:vmware:vcenter_server:*:*:*:*:*:*	CWE-264

Recommendations



Update: To mitigate this risk, it is essential to update to the patched versions of vCenter Server 8.0 U2d, 8.0 U1e, 7.0 U3r. Regularly check for updates and apply them promptly to ensure that your system is protected against known vulnerabilities.



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.



Limit Exposure: Configure firewalls to restrict access to the vCenter Server only to necessary services and IP addresses.



Vulnerability Management: Implement a robust vulnerability management process to ensure that software and systems are regularly assessed for vulnerabilities and updated with the required security patches. Prioritize critical vulnerabilities identified by security advisories and vendors to mitigate the risk of exploitation by threat actors.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	TA0004 Privilege Escalation
T1588 Obtain Capabilities	T1588.006 Vulnerabilities	T1190 Exploit Public-Facing Application	T1068 Exploitation for Privilege Escalation
T1059 Command and Scripting Interpreter	T1548 Abuse Elevation Control Mechanism	T1548.003 Sudo and Sudo Caching	

Patch Details

Updates addressing the vulnerabilities were made available in VMware vCenter Server versions 8.0 U2d, 8.0 U1e, and 7.0 U3r. For VMware Cloud Foundation, patches are provided through KB88287.

Links:

<https://docs.vmware.com/en/VMware-vSphere/8.0/rn/vsphere-vcenter-server-80u2d-release-notes/index.html>

<https://docs.vmware.com/en/VMware-vSphere/8.0/rn/vsphere-vcenter-server-80u1e-release-notes/index.html>

<https://docs.vmware.com/en/VMware-vSphere/7.0/rn/vsphere-vcenter-server-70u3r-release-notes/index.html>

<https://knowledge.broadcom.com/external/article?legacyId=88287>

References

<https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24453>

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

June 19, 2024 • 6:30 AM

© 2024 All Rights are Reserved by Hive Pro



More at www.hivepro.com