

HiveForce Labs

THREAT ADVISORY

 **VULNERABILITY REPORT**

Active Exploitation of vCenter Server Vulnerabilities

Date of Publication

November 19, 2024

Admiralty Code

A1

TA Number

TA2024435







Summary

First Seen: September 17, 2024

Affected Product: VMware vCenter Server

Impact: VMware's vCenter Server has two critical vulnerabilities (CVE-2024-38812 and CVE-2024-38813), both actively exploited in the wild. CVE-2024-38812 allows remote code execution via a heap overflow, while CVE-2024-38813 enables privilege escalation. VMware issued initial patches in September, but further updates were required due to incomplete fixes. Administrators should apply the latest patches immediately to mitigate these risks.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2024-38812	VMware vCenter Server Heap-Overflow Vulnerability	VMwarevCenter Server			
CVE-2024-38813	VMware vCenter Server Privilege Escalation Vulnerability	VMware vCenter Server			

Vulnerability Details

#1

VMware has disclosed two critical vulnerabilities, CVE-2024-38812 and CVE-2024-38813, in its vCenter Server software, which are being actively exploited in the wild. The first flaw, CVE-2024-38812, is a heap-overflow vulnerability in the Distributed Computing Environment/Remote Procedure Call (DCERPC) protocol. It allows attackers to execute arbitrary code remotely by sending crafted network packets. This flaw has been assigned a severity score of 9.8/10, making it particularly dangerous. Despite an initial patch released in September 2024, VMware later revealed that the fix was insufficient, prompting an urgent update.

#2

The second issue, CVE-2024-38813, is a privilege escalation vulnerability that enables attackers to gain root-level access to affected systems using similar crafted network packets. While it is less critical than CVE-2024-38812, it is often exploited in tandem with the latter, increasing the risk of full system compromise. Both vulnerabilities were initially identified during a Chinese hacking contest and have been exploited in attacks targeting VMware environments, including vSphere and VMware Cloud Foundation.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-38812	VMware vCenter Server: 7.0 - 8.0 VMware Cloud Foundation: 4.x - 5.1.x	cpe:2.3:a:vmware:vcenter_server:*:*:*:*:*:* cpe:2.3:a:vmware:cloud_foundation:*:*:*:*:*:* *.*	CWE-122
CVE-2024-38813	VMware vCenter Server: 7.0 - 8.0 VMware Cloud Foundation: 4.x - 5.1.x	cpe:2.3:a:vmware:vcenter_server:*:*:*:*:*:* cpe:2.3:a:vmware:cloud_foundation:*:*:*:*:*:* *.*	CWE-78

Recommendations



Immediate Patch Application: Ensure that the latest security updates released by VMware are applied as soon as possible. VMware has acknowledged that earlier patches were incomplete, and updated fixes are now available. These patches address the critical flaws, including remote code execution and privilege escalation vulnerabilities.



Snapshot Before Updates: Before applying any updates, create a non-memory snapshot of the vCenter Server Appliance (VCSA). This precaution allows you to revert the appliance to its pre-update state in case of any issues during the update process.



Segmentation and Network Access Control: Restrict network access to vCenter Server instances to trusted hosts only. Employ firewalls and network segmentation to minimize exposure to potential attackers.



Regular Updates and Maintenance: Beyond these vulnerabilities, ensure that all VMware software and other critical infrastructure systems are consistently updated. Regular maintenance reduces the risk of exploitation of newly discovered vulnerabilities.



Potential MITRE ATT&CK TTPs

<u>TA0040</u> Impact	<u>TA0042</u> Resource Development	<u>TA0002</u> Execution	<u>TA0004</u> Privilege Escalation
<u>T1059</u> Command and Scripting Interpreter	<u>T1588.006</u> Vulnerabilities	<u>T1588</u> Obtain Capabilities	<u>T1588.005</u> Exploits
<u>T1068</u> Exploitation for Privilege Escalation	<u>T1203</u> Exploitation for Client Execution		



Patch Links

<https://support.broadcom.com/web/ecx/solutiondetails?patchId=5574>

<https://support.broadcom.com/web/ecx/solutiondetails?patchId=5531>

<https://support.broadcom.com/web/ecx/solutiondetails?patchId=5580>

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



References

<https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24968>

<https://github.com/vmware/vcf-security-and-compliance-guidelines/blob/main/security-advisories/vmsa-2024-0019/README.md>

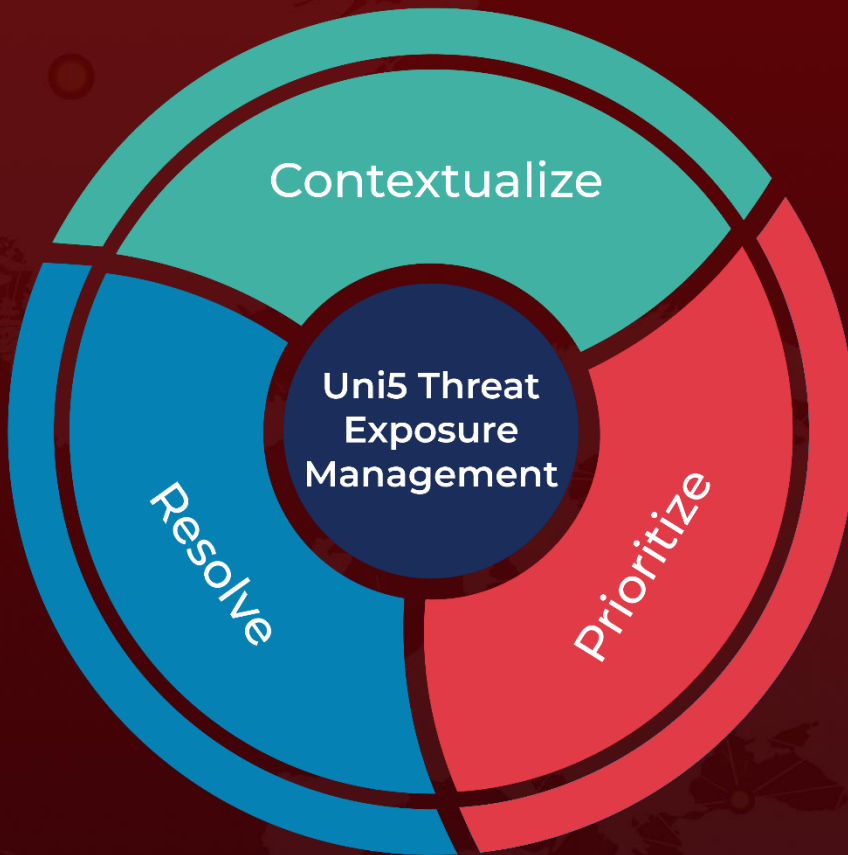
<https://github.com/groshi/CVE-2024-38812-POC-5-Hands-Private>



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

November 19, 2024 • 7:30 AM

© 2024 All Rights are Reserved by Hive Pro



More at www.hivepro.com