BLACKSWAN CYBERSECURITY

THREAT ADVISORY

September 23, 2024

Critical VMWare vCenter Server Flaw (CVE-2024-38812)

SUMMARY

Broadcom released a critical security update for VMware vCenter Server to address a high-severity vulnerability that could allow remote code execution (RECE). In addition to this CVE-2024-38812, another vulnerability that allows privilege escalation (CVE-2024-38813) has been patched. vCenter Server installations must be updated to the latest versions immediately.

RISK SCORE

CVE-ID	CVSSv3 Score
CVE-2024-38812	9.8
CVE-2024-38813	7.3

VULNERABILITY DETAILS

Broadcom issued a security patch for VMware vCenter Server to mitigate the critical vulnerability CVE-2024-38812. This heap-overflow vulnerability in the DCE/RPC protocol potentially allows a malicious actor to exploit this flaw in low-complexity attacks that don't require user interaction by sending specially crafted network packets, leading to remote code execution.

Broadcom also provided a patch for a privilege escalation vulnerability (CVE-2024-38813) with a CVSS score of 7.5, which could allow an attacker to escalate privileges to root. This flaw, along with CVE-2024-38812, was discovered by security researchers from Team TZL during the Matrix Cup cybersecurity competition in June 2024.

AFFECTED PRODUCTS

- vCenter Server versions 7.0 and 8.0
- VMware Cloud Foundation versions 4.x and 5.x

SOLUTION

- vCenter Server 8.0: Fixed in version 8.0 U3b
- vCenter Server 7.0: Fixed in version 7.0 U3s
- VMware Cloud Foundation 5.x: Fixed in 8.0 U3b as an asynchronous patch
- VMware Cloud Foundation 4.x: Fixed in 7.0 U3s as an asynchronous patch

RECOMMENDATIONS

- Update vCenter Server and VMware Cloud Foundation to the latest versions as specified above.
- Regularly monitor systems for potential exploits and ensure that only trusted network connections are allowed to access vCenter services.

- Strictly control network perimeter access to vSphere management components and interfaces, including storage and network components.

REFERENCES

- https://thehackernews.com/2024/09/patch-issued-for-critical-vmware.html
- https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24968
- https://www.bleepingcomputer.com/news/security/broadcom-fixes-critical-rce-bug-in-vmware-vcenter-server/