



مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



Security Updates- VMware Products

Tracking #:432316299

Date:18-09-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that VMware released a security advisory (VMSA-2024-0019) addressing critical vulnerabilities in VMware vCenter Server and VMware Cloud Foundation.

TECHNICAL DETAILS:

On September 17, 2024, VMware released a security advisory (VMSA-2024-0019) addressing critical vulnerabilities in VMware vCenter Server and VMware Cloud Foundation. The vulnerabilities, identified as CVE-2024-38812 and CVE-2024-38813, pose significant risks, including potential remote code execution and privilege escalation.

Vulnerability Overview:

- **CVE-2024-38812:** A heap-overflow vulnerability in the DCERPC protocol implementation allows remote attackers with network access to execute arbitrary code by sending specially crafted packets. This vulnerability has been assigned a **CVSS score of 9.8**, indicating its critical nature.
- **CVE-2024-38813:** A privilege escalation vulnerability enables an attacker with network access to escalate their privileges to root on the vCenter Server Appliance by exploiting crafted packets. This vulnerability carries a CVSS score of 7.5.

VMware Product	Version	Running On	CVE	CVSSv3	Severity	Fixed Version
vCenter Server	8	Any	CVE-2024-38812, CVE-2024-38813	9.8, 7.5	Critical	8.0 U3b
vCenter Server	7	Any	CVE-2024-38812, CVE-2024-38813	9.8, 7.5	Critical	7.0 U3s
VMware Cloud Foundation	5.x	Any	CVE-2024-38812, CVE-2024-38813	9.8, 7.5	Critical	Async patch to 8.0 U3b
VMware Cloud Foundation	4.x	Any	CVE-2024-38812, CVE-2024-38813	9.8, 7.5	Critical	Async patch to 7.0 U3s

RECOMMENDATIONS:

- Apply the latest updates as soon as possible and verify that the vulnerabilities have been successfully mitigated.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.



REFERENCES:

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