مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerabilities in VMware vCenter Server

Tracking #:432316425

Date:22-10-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed VMware has released critical updates to address two significant vulnerabilities in vCenter Server.

TECHNICAL DETAILS:

VMware has released critical updates to address two significant vulnerabilities in vCenter Server: a heap-overflow vulnerability (**CVE-2024-38812**) with a CVSSv3 score of 9.8, and a privilege escalation vulnerability (**CVE-2024-38813**) with a CVSSv3 score of 7.5. These vulnerabilities can potentially allow an attacker with network access to execute arbitrary code or escalate privileges to root, posing severe risks to affected systems.

Vulnerability Details:

1. **Heap-Overflow Vulnerability (CVE-2024-38812)**
   - **Description**: This vulnerability exists in the DCERPC protocol implementation within vCenter Server, allowing for remote code execution.
   - **Impact**: An attacker can exploit this by sending a specially crafted network packet, leading to potential system compromise.
   - **Severity**: Critical (CVSSv3 score: 9.8)
   - **Resolution**: Apply the updates listed in the Response Matrix for affected deployments.
2. **Privilege Escalation Vulnerability (CVE-2024-38813)**
   - **Description**: This vulnerability allows an attacker with network access to escalate privileges to root by sending crafted network packets.
   - **Impact**: Successful exploitation can lead to unauthorized access and control over the system.
   - **Severity**: Important (CVSSv3 score: 7.5)
   - **Resolution**: Apply the updates listed in the Response Matrix for affected deployments.

Important Information:

- VMware has acknowledged that the initial patches released on September 17 did not fully address CVE-2024-38812, making it critical for users to apply the latest updates.
- There are no known workarounds for these vulnerabilities; hence, patching is essential.

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 U3d, 8.0 U2e
vCenter Server	7	Any	CVE-2024-38812, CVE-2024-38813	9.8, 7.5	Critical	7.0 U3t
VMware Cloud Foundation	5.x	Any	CVE-2024-38812, CVE-2024-38813	9.8, 7.5	Critical	Async patch to 8.0 U3d
VMware Cloud Foundation	5.1.x	Any	CVE-2024-38812, CVE-2024-38813	9.8, 7.5	Critical	Async patch to 8.0 U2e

VMware Cloud Foundation	4.x	Any	CVE-2024-38812, CVE-2024-38813	9.8, 7.5	Critical	Async patch to 7.0 U3t

RECOMMENDATIONS:

- **Immediate Action**: All customers using VMware vCenter Server or VMware Cloud Foundation are urged to apply the latest patches as soon as possible.
- **Monitoring and Detection**: Implement monitoring solutions to detect any suspicious activity related to these vulnerabilities.

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