مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

VMware Security Updates

Tracking #:432315962

Date:19-06-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that VMware released security updates to patch critical vulnerabilities in VMware vCenter Server and VMware Cloud Foundation products.

TECHNICAL DETAILS:

Vulnerabilities Details:

- **CVE-2024-37079 & CVE-2024-37080 (Critical Severity - CVSS v3 score: 9.8)**
  - Multiple heap-overflow vulnerabilities exist in the DCERPC protocol implementation of vCenter Server.
  - A remote attacker with network access can exploit these vulnerabilities to execute arbitrary code on the affected system.
- **CVE-2024-37081 (High Severity - CVSS v3 score: 7.8)**
  - Multiple privilege escalation vulnerabilities arise due to misconfiguration of the sudo utility on vCenter Server Appliance.
  - An authenticated local user with non-administrative privileges can exploit this vulnerability to gain root access on the system.

VMware Product	Version	CVE	Fixed Version
vCenter Server	8	CVE-2024-37079, CVE-2024-37080, CVE-2024-37081	8.0 U2d
vCenter Server	8	CVE-2024-37079, CVE-2024-37080	8.0 U1e
vCenter Server	7	CVE-2024-37079, CVE-2024-37080, CVE-2024-37081	7.0 U3r
Cloud Foundation (vCenter Server)	5.x	CVE-2024-37079, CVE-2024-37080, CVE-2024-37081	KB88287
Cloud Foundation (vCenter Server)	4.x	CVE-2024-37079, CVE-2024-37080, CVE-2024-37081	KB88287

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by VMware.

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/0/24453