مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Multiple Vulnerabilities in VMware Products

Tracking #:432316399

Date:16-10-2024

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed multiple vulnerabilities in VMware NSX and VMware Cloud Foundation that could be exploited to gain unauthorized access to systems and potentially compromise sensitive data.

TECHNICAL DETAILS:

Vulnerability Details:

1. **CVE-2024-38817: Command Injection Vulnerability**
   - **Severity:** Moderate (CVSSv3: 6.7)
   - **Description:** This vulnerability allows an attacker with access to the NSX Edge CLI terminal to execute arbitrary commands on the underlying operating system as root.
2. **CVE-2024-38818: Local Privilege Escalation Vulnerability**
   - **Severity:** Moderate (CVSSv3: 6.7)
   - **Description:** An authenticated attacker can exploit this vulnerability to elevate their privileges and gain access to resources they are not normally authorized to use.
3. **CVE-2024-38815: Content Spoofing Vulnerability**
   - **Severity:** Moderate (CVSSv3: 4.3)
   - **Description:** An unauthenticated attacker can craft malicious URLs to redirect users to malicious websites, potentially leading to data exfiltration or other attacks.

Affected Products:

- VMware NSX
- VMware Cloud Foundation

Fixed Versions:

- NSX 4.2.1
- NSX-T 3.2.4.1
- Cloud Foundation (NSX) Async Patch to 4.2.1
- Cloud Foundation (NSX-T) Async Patch to 3.2.4.1

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to upgrade the affected versions to the fixed versions at the earliest.

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/0/25047