مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Multiple Vulnerabilities in NetApp Products

Tracking #:432316524

Date:18-11-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has obsrved multiple vulnerabilities in NetApp products that could potentially be exploited to allow unauthorized access, privilege escalation, or denial of service on affected systems.

TECHNICAL DETAILS:

Critical-Severity Vulnerabilities:

- CVE-2024-29736 Apache CXF Vulnerability in NetApp Products
- CVE-2022-0318 Vim Vulnerability in NetApp Products
- CVE-2024-38428 GNU Wget Vulnerability in NetApp Products
- CVE-2023-24538 Golang Vulnerability in NetApp Products
- CVE-2023-24540 Golang Vulnerability in NetApp Products
- CVE-2023-29404 Golang Vulnerability in NetApp Products
- CVE-2022-3520 Vim Vulnerability in NetApp Products

High-Severity Vulnerability:

- CVE-2024-25744 Linux Kernel Vulnerability in NetApp Products

Successful exploitations of These vulnerabilities could potentially allow attackers to execute arbitrary code, escalate privileges, or cause other serious security issues in affected NetApp systems. The specific impact may vary depending on the vulnerability and the affected product.

Note: Refer to NetApp advisories for affected products, mitigations and more information.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the mitigation or workaround provided by NetApp.

Apply Patches: As soon as patches or updates become available, apply them to all affected systems. Prioritize applying patches for critical severity 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://security.netapp.com/advisory/ntap-20241115-0003/
- https://security.netapp.com/advisory/ntap-20241115-0004/
- https://security.netapp.com/advisory/ntap-20241115-0005/
- https://security.netapp.com/advisory/ntap-20241115-0006/
- https://security.netapp.com/advisory/ntap-20241115-0007/
- https://security.netapp.com/advisory/ntap-20241115-0008/

- https://security.netapp.com/advisory/ntap-20241115-0009/
- https://security.netapp.com/advisory/ntap-20241115-0010/