مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Multiple Vulnerabilities in NetApp Products

Tracking #:432316413

Date:21-10-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed multiple vulnerabilities in NetApp products that could be exploited to achieve remote code execution, denial of service, and other serious security breaches on affected systems.

TECHNICAL DETAILS:

Critical-Severity Vulnerabilities:

- CVE-2024-45491 libexpat Vulnerability in NetApp Products
- CVE-2024-45490 libexpat Vulnerability in NetApp Products
- CVE-2024-45492 libexpat Vulnerability in NetApp Products

High-Severity Vulnerabilities:

- CVE-2024-36883 Linux Kernel Vulnerability in NetApp Products
- CVE-2024-36886 Linux Kernel Vulnerability in NetApp Products
- CVE-2024-7592 Python Vulnerability in NetApp Products
- CVE-2024-6232 Python Vulnerability in NetApp Products

Successful exploitation of these vulnerabilities could lead to:

- Unauthorized access to sensitive data
- Remote code execution
- Denial of service (DoS) attacks

Note: Refer to NetApp advisories for 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/