مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Multiple Vulnerabilities in NetApp Products

Tracking #:432316344

Date:30-09-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed multiple vulnerabilities in NetApp products that could be exploited to cause denial of service (DoS), disclose sensitive information, or allow unauthorized data modification on affected systems.

TECHNICAL DETAILS:

Vulnerabilities Details:

1. **CVE-2024-45287: FreeBSD Denial of Service Vulnerability**
   - **Severity:** High (CVSS Score: 7.5)
   - All supported versions of FreeBSD, which is incorporated into ONTAP 9, are susceptible to a vulnerability that could be exploited to cause a denial of service.
2. **CVE-2024-34156: Golang Denial of Service Vulnerability**
   - **Severity:** High (CVSS Score: 7.5)
   - Golang versions prior to 1.22.7 and 1.23.0-0 prior to 1.23.1 are vulnerable to a denial of service attack. Multiple NetApp products incorporate Golang.
3. **CVE-2023-30583: Node.js Information Disclosure Vulnerability**
   - **Severity:** High (CVSS Score: 7.5)
   - Node.js versions 20.x prior to 20.3.1 are susceptible to a vulnerability that could lead to the disclosure of sensitive information. Multiple NetApp products incorporate Node.js.
4. **CVE-2024-45409: Ruby SAML Critical Vulnerability**
   - **Severity:** Critical (CVSS Score: 9.8)
   - Certain versions of Ruby-SAML, which is used in multiple NetApp products, are vulnerable to a critical vulnerability that could lead to the disclosure of sensitive information, unauthorized data modification, or a denial of service.

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.

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-20240926-0010/
- https://security.netapp.com/advisory/ntap-20240926-0004/
- https://security.netapp.com/advisory/ntap-20240926-0006/
- https://security.netapp.com/advisory/ntap-20240926-0008/