مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerability in Synology DiskStation Manager (DSM)

Tracking #:432318633

Date:21-03-2026

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability in the telnetd component of GNU Inetutils used in Synology DiskStation Manager (DSM). CVE-2026-32746 allows unauthenticated remote attackers to execute arbitrary commands, potentially leading to full system compromise.

TECHNICAL DETAILS:

Vulnerability Details

- **CVE ID:** CVE-2026-32746
- **Severity:** Critical **CVSS 3.1 Base Score:** 9.8
- **CWE:** CWE-120 – Buffer Copy without Checking Size of Input
- The telnetd service in GNU Inetutils versions through 2.7 is vulnerable to an out-of-bounds write in the LINEMODE SLC (Set Local Characters) suboption handler. The add_slc function does not check whether the buffer is full, allowing remote attackers to execute arbitrary code without authentication.

Affected Products and Fixed Versions

- **DSM 7.3:** Upgrade to 7.3.2-86009-3 or above
- **DSM 7.2.2:** Upgrade to 7.2.2-72806-8 or above
- **DSM 7.2.1:** Upgrade to 7.2.1-69057-11 or above
- **DSMUC 3.1:** Fixed version ongoing

Mitigation

- Disable the Telnet service until patches can be applied:
  Navigate to **Control Panel > Terminal**, uncheck **Enable Telnet service**, and click **Apply**.

RECOMMENDATIONS:

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

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://www.synology.com/en-global/security/advisory/Synology_SA_26_03