NATIONAL CSIRT-CY

Multiple Vulnerabilities in **Synology DSM**

20 April 2026

[Cyber Threat Intelligence]

EXECUTIVE SUMMARY:

The Digital Security Authority (DSA) wants to bring to your attention multiple vulnerabilities in **Synology DiskStation Manager (DSM)** that could allow attackers to read or modify files, access sensitive information, and perform denial-of-service (DoS) attacks.

TECHNICAL DETAILS:

Vulnerability Details

• **CVE-2026-40530** – Important (CVSS 8.0) CRLF Injection vulnerability allowing arbitrary file read/write and DoS.
• **CVE-2026-40539** – Important (CVSS 7.1) Improper certificate validation enabling man-in-the-middle (MITM) attacks.
• **CVE-2026-4036** – Moderate (CVSS 6.5) SQL Injection vulnerability leading to sensitive data exposure.
• **CVE-2026-40531 / 40532 / 40534 / 40536 / 40537** – Moderate (CVSS 4.3–6.5) Includes Integer Overflow, Forced Browsing, Cross-Site Scripting (XSS), Path Traversal, and SSRF vulnerabilities.
• **CVE-2026-40533 / 40535 / 40538** – Low to Moderate (CVSS 3.7–6.5) Information disclosure, Path Traversal, and improper authentication attempt restrictions.

These vulnerabilities may allow remote authenticated or unauthenticated attackers to:

• Read or write arbitrary or limited files
• Access sensitive or non-sensitive data
• Execute limited or full denial-of-service attacks
• Exploit MITM conditions in certain scenarios

Fixed Versions

• DSM 7.3 → Upgrade to **7.3.2-86009-2 or above**
• DSM 7.2.2 → Upgrade to **7.2.2-72806-7 or above**
• DSM 7.2.1 → Upgrade to **7.2.1-69057-10 or above**

RECOMMENDATIONS:

The Digital Security Authority (DSA) recommends applying the mitigation or workaround provided by Synology.

Please ensure to distribute this information among your subsidiaries and partners and provide us with any pertinent information or findings you may have (such as Indicators of Compromise, Tactics, Techniques, and Procedures, etc.).

The Digital Security Authority (DSA) extends its appreciation for the continued collaboration.

REFERENCES:

1. https://nvd.nist.gov/vuln/detail/CVE-2026-3324 · Security Note

DISCLAIMER:

The information presented in this report is based on available data up to the 20th of April 2024.

Organizations are advised to consult with relevant cybersecurity professionals and follow best practices for their specific environments.