مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Multiple Vulnerabilities in Synology BeeStation

Tracking #:432318096

Date:04-12-2025

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed multiple vulnerabilities in Synology BeeStation devices that, when exploited in sequence, could allow an unauthenticated remote attacker to achieve full system compromise.

TECHNICAL DETAILS:

Multiple vulnerabilities have been identified in Synology BeeStation devices that, when exploited in sequence, allow an unauthenticated remote attacker to achieve full system compromise, including remote code execution with root privileges. The exploitation chain leverages a CRLF injection flaw, an authentication bypass, and a SQL injection vulnerability to escalate from information disclosure to complete system takeover. A public proof-of-concept (PoC) exploit is available.

Vulnerability Details
CVE-2024-50629 – CRLF Injection

- **CVSS Score:** 5.3 (Medium)
- A CRLF injection vulnerability exists in the redirect_url parameter of the BeeStation authentication API. The lack of input sanitization allows the injection of arbitrary HTTP headers. Through this flaw, attackers can force the server to expose internal files, including system logs that reveal sensitive information such as valid usernames. This serves as the initial foothold in the exploit chain.

CVE-2024-50630 – Improper Authentication

- **CVSS Score:** 7.5 (High)
- A logic flaw in the syncd daemon enables authentication bypass. By submitting a request without the password parameter, the system erroneously interprets it as a trusted local socket request. This results in the issuance of a valid access token based solely on the leaked username obtained in the previous step, allowing unauthorized access.

CVE-2024-50631 – SQL Injection

- **CVSS Score:** 7.5 (High)
- The update_settings function is vulnerable to SQL Injection, enabling attackers to manipulate SQLite operations and write arbitrary files to system directories. Using the ATTACH DATABASE command, an attacker can create a malicious file in /etc/cron.d/. Despite binary data in the file, the cron daemon ignores malformed lines and executes valid entries, allowing the execution of arbitrary commands as root. This completes the exploit chain and provides full remote code execution.

Impact
Successful exploitation of these vulnerabilities can result in a complete compromise of affected BeeStation devices. An attacker could gain unauthorized access to sensitive system resources and user data, escalate privileges to root, execute arbitrary commands, and create or modify scheduled tasks for persistent access. This could ultimately allow full remote control of the device, enabling deployment of malicious payloads, data exfiltration, or disruption of services.

Affected Versions:

- DSM: < 7.2.2-72806-1
- BSM: < 1.1-65374

- Synology Drive Server: < 3.5.1-26102

Fixed Versions:

- DSM 7.2.2 – Upgrade to 7.2.2-72806-1 or above
- DSM 7.2.1 – Upgrade to 7.2.1-69057-6 or above
- DSM 7.2 – Upgrade to 7.2-64570-4 or above
- DSM 7.1 – Upgrade to 7.1.1-42962-7 or above
- DSM 6.2 – Upgrade to 6.2.4-25556-8 or above
- Synology Drive Server for DSM 7.2.2 – Upgrade to 3.5.1-26102 or above
- Synology Drive Server for DSM 7.2.1 – Upgrade to 3.5.0-26085 or above
- Synology Drive Server for DSM 7.1 – Upgrade to 3.2.1-23280 or above
- Synology Drive Server for DSM 6.2 – Upgrade to 3.0.4-12699 or above

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-us/security/advisory/Synology_SA_24_20
- https://www.synology.com/en-us/security/advisory/Synology_SA_24_21
- https://www.synology.com/en-us/security/advisory/Synology_SA_24_21
- https://kiddo-pwn.github.io/blog/2025-11-30/writing-sync-popping-cron