



مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



Security Updates - Synology DSM and BeeDrive
Tracking #:432316572
Date:28-11-2024

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 INTELLIGENCE 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 that Synology has released security updates to patch multiple vulnerabilities in DSM (DiskStation Manager) and BeeDrive for desktop.

TECHNICAL DETAILS:

Synology has released important security updates addressing multiple vulnerabilities in DSM (DiskStation Manager) and BeeDrive for desktop.

Vulnerabilities Details:

- **DSM Vulnerabilities (Synology-SA-24:27)**
 - Severity: Important
 - **Denial-of-Service Vulnerability:** Remote attackers can potentially conduct denial-of-service attacks, disrupting system availability.
 - **Information Disclosure Vulnerability:** Remote attackers may be able to obtain sensitive information, compromising data confidentiality.
 - **Privilege Escalation Vulnerability:** Remote authenticated users could potentially obtain elevated privileges without proper authorization.
- **BeeDrive for Desktop Vulnerabilities (Synology-SA-24:26)**
 - **Severity: Important**
 - **Arbitrary Code Execution:** Local users may be able to execute arbitrary code, potentially compromising system integrity.
 - **Denial-of-Service Vulnerability:** Local users could conduct denial-of-service attacks, affecting system availability.

Affected Versions	Fixed Release Availability
DSM 7.2.2	Upgrade to 7.2.2-72806 or above.
DSM 7.2.1	Upgrade to 7.2.1-69057-2 or above.
DSM 7.1	Updates ongoing, check for latest version
DSMUC 3.1	Upgrade to 3.1.4-23079 or above.
BeeDrive for desktop	Upgrade to 1.3.2-13814 or above.

RECOMMENDATIONS:

- **Immediate Updates:**
 - For products with available fixes, update to the specified versions immediately.
 - For products marked as "Ongoing," monitor Synology's official channels for update releases.

- Regularly check for and apply software updates.
- Monitor Synology's official security advisories for further information.

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-my/security/advisory/Synology_SA_24_26
- https://www.synology.com/en-my/security/advisory/Synology_SA_24_27