



مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



Critical Vulnerabilities in Synology Products

Tracking #:432316479

Date:06-11-2024

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 multiple critical vulnerabilities in Synology products that could be exploited by malicious actors to compromise affected systems, potentially leading to data breaches, system disruptions, and unauthorized access.

TECHNICAL DETAILS:

Vulnerabilities Details:

- **Synology-SA-24:20 DSM**
 - Severity: **Critical**
 - Multiple vulnerabilities in Synology DiskStation Manager (DSM). These vulnerabilities allow for remote code execution, man-in-the-middle attacks, and unauthorized file access, posing significant risks to affected systems.
- **Synology-SA-24:21 Synology Drive Server**
 - Severity: Important
 - Multiple vulnerabilities in Synology Drive Server. These vulnerabilities could allow remote attackers to hijack web sessions and inject SQL commands via a susceptible version of Synology Drive Server.
- **Synology-SA-24:22 Replication Service**
 - Severity: **Critical**
 - A vulnerability in Replication Service enables remote attackers to execute arbitrary commands on vulnerable systems.
- **Synology-SA-24:23 BeeStation**
 - Severity: **Critical**
 - Multiple vulnerabilities in BeeStation. These vulnerabilities could allow remote attackers to execute arbitrary code, read specific files, and enable adjacent man-in-the-middle attackers to write specific files on vulnerable systems.

Affected Product	Fixed Release Availability
DSM 7.2	Upgrade to 7.2.2-72806-1 or above.
DSM 7.1	Ongoing
DSMUC 3.1	Ongoing
Synology Drive Server for DSM 7.2	Upgrade to 3.5.1-26102 or above.
Synology Drive Server for DSM 7.1	Ongoing
Replication Service for DSM 7.2	Upgrade to 1.3.0-0423 or above.
Replication Service for DSM 7.1	Upgrade to 1.2.2-0353 or above.
BeeStation OS 1.1	Upgrade to 1.1-65374 or above.
BeeStation OS 1.0	Upgrade to 1.1-65374 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.
- Implement comprehensive security measures to protect against potential exploits.

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_20
- https://www.synology.com/en-my/security/advisory/Synology_SA_24_21
- https://www.synology.com/en-my/security/advisory/Synology_SA_24_22
- https://www.synology.com/en-my/security/advisory/Synology_SA_24_23