مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerabilities in Synology Products

Tracking #:432316416

Date:21-10-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed critical vulnerabilities in Synology products that could be exploited to gain unauthorized access, execute malicious code, and disrupt services on affected systems.

TECHNICAL DETAILS:

Critical-Severity Vulnerabilities:

- **Synology-SA-24:17 Synology Camera**
  - Remote attackers can exploit these vulnerabilities to execute arbitrary code, bypass security constraints, and initiate denial-of-service attacks. This could lead to unauthorized access and potential device inoperability.
- **Synology-SA-24:15 BeeStation**
  - A vulnerability exists that allows remote attackers to execute arbitrary code via susceptible versions of Synology BeeStation Manager (BSM).
- **Synology-SA-24:12 GitLab**
  - A vulnerability allows remote attackers to bypass authentication mechanisms in susceptible versions of GitLab.

Affected Product	Fixed Versions
Synology Camera BC500 Firmware	Upgrade to 1.1.3-0442 or above.
Synology Camera CC400W Firmware	Upgrade to 1.1.3-0442 or above.
Synology Camera TC500 Firmware	Upgrade to 1.1.3-0442 or above.
BeeStation OS 1.1	Upgrade to 1.1-65373 or above.
GtiLab for DSM 6.2	Upgrade to 13.12.2-0074 or above

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to upgrade the affected versions to the fixed versions at the earliest.

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