مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

Critical Vulnerability in Synology Gitlab DSM

Tracking #:432316378

Date:09-10-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Synology released an advisory regarding a critical vulnerability (CVE-2024-45409) affecting GitLab for DSM 6.2.

TECHNICAL DETAILS:

On October 9, 2024, Synology released an advisory regarding a critical vulnerability (**CVE-2024-45409**) affecting GitLab for DSM 6.2. This vulnerability allows unauthenticated remote attackers to bypass authentication and gain unauthorized access to the system.

Details of the Vulnerability

- **CVE Identifier**: CVE-2024-45409
- **Severity**: Critical
- **CVSS3 Base Score**: 9.1

Description:

The vulnerability stems from the Ruby SAML library used in GitLab, specifically versions up to 12.2 and 1.13.0 through 1.16.0. The library fails to properly verify the signature of SAML Responses, allowing an unauthenticated attacker with access to any signed SAML document from the Identity Provider (IdP) to forge a SAML Response or Assertion with arbitrary contents. This enables the attacker to log in as any user within the vulnerable system.

Fixed Release:

- GitLab for DSM 6.2- Upgrade to 13.12.2-0074 or above

RECOMMENDATIONS:

- Users must upgrade their GitLab installations to fixed version as soon as possible.
- Regularly monitor access logs for any unauthorized access attempts and audit user accounts for anomalies.

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-me/security/advisory/Synology_SA_24_12