مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates - GitLab

Tracking #:432316628

Date:12-12-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that GitLab has released security updates to address multiple vulnerabilities in Community Edition (CE) and Enterprise Edition (EE). These vulnerabilities could potentially lead to various security risks, including session data exfiltration, denial of service, information disclosure, and cross-site scripting.

TECHNICAL DETAILS:

GitLab has released security updates to address multiple vulnerabilities in its Community Edition (CE) and Enterprise Edition (EE). These vulnerabilities affect various versions of GitLab and pose significant security risks.

High-Severity Vulnerabilities:

- Network Error Logging (NEL) Header Injection (CVE-2024-11274)
  - CVSS Score: 8.7
  - An attacker could inject Network Error Logging (NEL) headers in Kubernetes proxy responses, potentially leading to session data exfiltration and account takeover (ATO) through OAuth flow abuse.
- Denial of Service via Diff-File Requests (CVE-2024-8233)
  - CVSS Score: 7.5
  - An unauthenticated attacker could cause a denial of service by repeatedly sending requests for diff files on commits or merge request.

Fixed Versions:

- GitLab Patch Release: 17.6.2, 17.5.4, 17.4.6 for GitLab Community Edition (CE) and Enterprise Edition (EE).

Note: Refer to Gitlab Advisory for Affected Versions and additional information.

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://about.gitlab.com/releases/2024/12/11/patch-release-gitlab-17-6-2-released/