U UNISPHERE SOLUTIONS

✉ info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 0321

GITLAB PATCHES 10.0 CRITICAL SEVERITY FLAW

DATE ISSUED: 1st June 2023

IMPACT	LOW	MEDIUM	[✓ HIGH]
EASE OF EXPLOIT	HARD	[✓ MEDIUM]	EASY

OVERVIEW

GitLab has released an emergency security update that patches a maximum severity path traversal flaw that could allow an unauthenticated attacker to read arbitrary files on the server when an attachment exists in a public project nested within at least five groups.

BREAKDOWN

GitLab is a web-based Git repository for developer teams that need to manage their code remotely. A researcher named 'pwnie' has reported a critical severity path traversal flaw in GitLab tracked as CVE-2023-2825 with a CVSS score of 10.0. A path traversal or directory traversal flaw allows an attacker to access files on the web server without proper authorization. The issue relates to how GitLab manages or resolves paths for attached files nested within several levels of the group hierarchy. Successful exploitation of this flaw could expose sensitive information, including proprietary software code, user credentials, tokens, and other critical system files. However, the vulnerability can only be exploited when there's an attachment in a public project nested within at least five groups, which is not the structure followed in all GitHub projects. The security flaw is discovered in GitLab Community Edition (CE) and Enterprise Edition (EE) version 16.0.0; however, older versions aren't affected. Due to the critical nature of this vulnerability, GitLab strongly recommends applying the latest security update as soon as possible.

REMEDIATION STEPS

- Update GitLab 16.0.0 to version 16.0.1 as soon as possible to mitigate the risk.
- Avoid relying on user-supplied input to make calls to the filesystem.
- Run the web server from a separate disk from your system disk and, if possible, don't store any sensitive files in the web server disk.
- Implement an Access Control List to control filesystem permissions.

REFERENCES & RESOURCES

Bleeping Computer	https://www.bleepingcomputer.com/news/security/gitlab-strongly-recommends-patching-max-severity-flaw-asap/
Gitlab	https://about.gitlab.com/releases/2023/05/23/critical-security-release-gitlab-16-0-1-released/
OWASP	https://owasp.org/www-community/attacks/Path_Traversal