

CVE-2023-7028

GitLab Community and Enterprise Editions Improper Access Control Vulnerability

Exigent CISA KEV since May 1, 2024 Actively exploited Public exploit module (Metasploit)

An issue has been discovered in GitLab CE/EE affecting all versions from 16.1 prior to 16.1.6, 16.2 prior to 16.2.9, 16.3 prior to 16.3.7, 16.4 prior to 16.4.5, 16.5 prior to 16.5.6, 16.6 prior to 16.6.4, and 16.7 prior to 16.7.2 in which user account password reset emails could be delivered to an unverified email address.

EVRS 86/100 Immediate priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.945 99.86th percentile · FIRST	CISA DEADLINE May 22, 2024 KEV since 2024 · listed over a year
--	--	---	--

Signals behind the score

☒ counted in the score ☐ not counted evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.945 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Out-of-band / urgent Patch or fixed version identified

CISA required action: Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.
Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
gitlab	≥ 16.1.0 < 16.1.6 ≥ 16.2.0 < 16.2.9 ≥ 16.3.0 < 16.3.7 ≥ 16.4.0 < 16.4.5 ≥ 16.5.0 < 16.5.6 ≥ 16.6.0 < 16.6.4 ≥ 16.7.0 < 16.7.2	16.1.6 · 16.2.9 · 16.3.7 · 16.4.5 · 16.5.6 · 16.6.4	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-mgg5-84cv-fc3c	Additional guidance	gitlab.com/gitlab-org/gitlab/-/issues/436084
about.gitlab.com	about.gitlab.com/releases/2024/01/11/critical-security-release-gitlab-16-7-2-released/	NVD	nvd.nist.gov/vuln/detail/CVE-2023-7028
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2023-59219
Current data	evulnable.com/vulnerability-management/cve/CVE-2023-7028		

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.