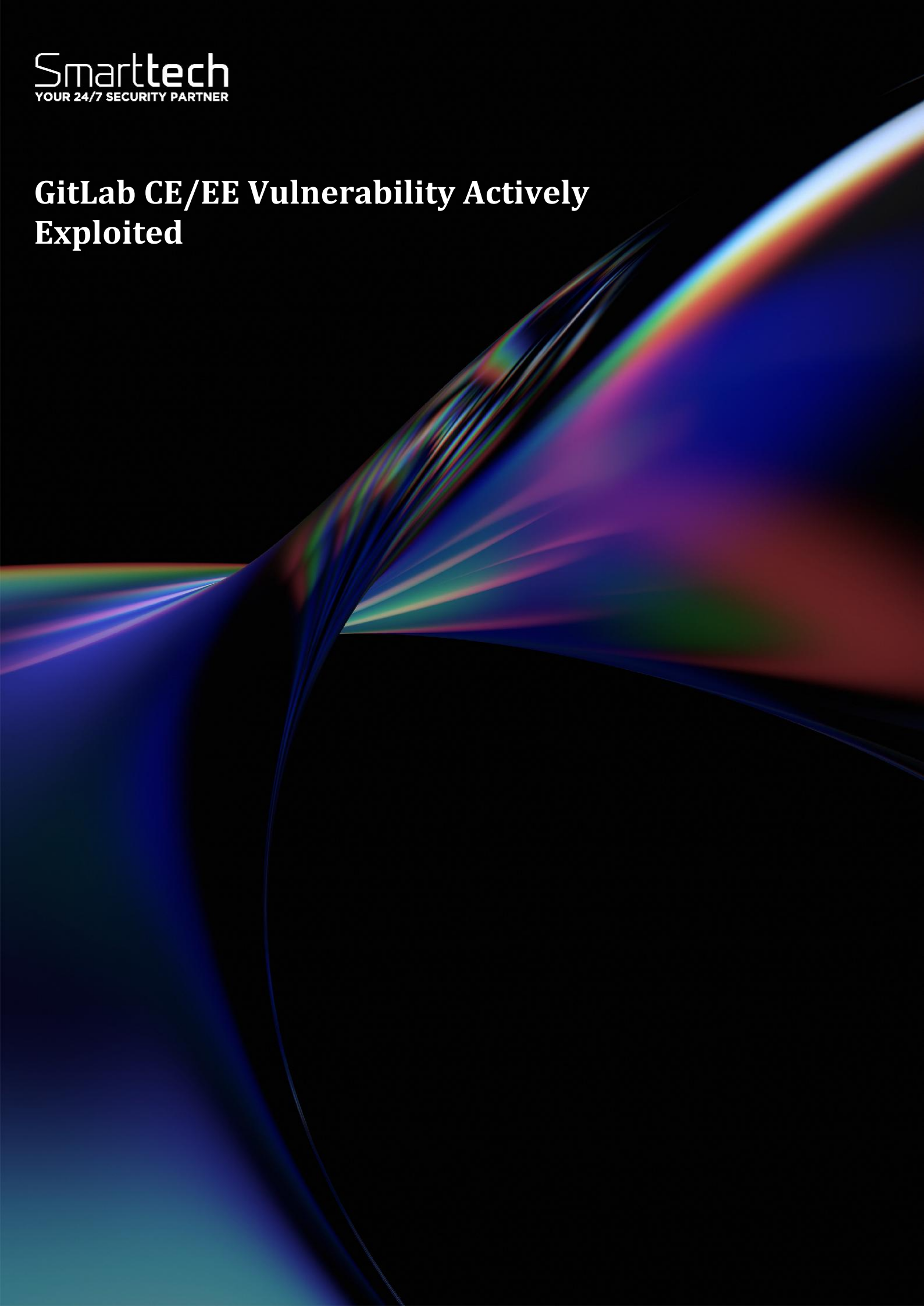
Smarttech
YOUR 24/7 SECURITY PARTNER

GitLab CE/EE Vulnerability Actively Exploited



Smarttech
YOUR 24/7 SECURITY PARTNER

Document ID	SMA-Threat Report
Document status	ISSUED
Issue Number	161
Authors	Dorin Constantin Banu < constatin.banu@smarttech247.com >
Verified by	Alin Curcan < alin.curcan@smarttech247.com >
Last modified	2026-09-14
Issue Date	2026-09-11

Threat Reports are reports created by Smarttech247 based on high and critical severity vulnerabilities that may have a high potential to be exploited in the wild i.e. vulnerabilities that are present in most used products by companies and do not have an auto-update option or they are usually not automatically updated in case that could lead to some service disruption. This report is usually created as soon as the vulnerability is released, therefore we strongly recommend that the information is reviewed, tests are performed and patches are applied before the first proof-of-concept is released. Even though certain vulnerabilities may not have an active exploit in the wild at the time that we report on them, we take into consideration the wider risk and the impact it could have on systems, should an exploit like that be available after a while. Our duty is to report them on time and we recommend enterprises that, in order to keep critical business systems protected, they should consider, on average, ten working days to check whether or not the new vulnerability affects them, and if so, to implement actions in order to remove the risk.

Overview:

A critical path traversal vulnerability in GitLab CE/EE is being actively exploited in the wild. Tracked as CVE-2026-85706, this flaw stems from improper path confinement combined with missing authentication enforcement in the affected API endpoint. Successful exploitation could allow an unauthenticated attacker to read arbitrary files from vulnerable GitLab servers and obtain sensitive information.

Risk

Government:

- Large and medium government entities: **Critical**
- Small government entities: **Critical**

Businesses:

- Large and medium business entities: **Critical**
- Small business entities: **Critical**

Technical summary

More details related to this vulnerability are as follows:

CVE ID	Description
CVE-2026-85706 **CVSS Base Score: 10**	GitLab has remediated an issue that, under certain conditions, an unauthenticated user could have read arbitrary files from the GitLab server due to improper path confinement and missing authentication enforcement in the repository commits API. Potential indicators of exploitation include HTTP POST requests to "/api/v4/projects/{id}/repository/commits/" containing the "file.path" parameter.

Affected Products

Product	Affected Version
GitLab	18.7 through 19.1.7
	19.2 through 19.2.5
	19.3 through 19.3.1

Recommendations

Smarttech247 team recommend the following actions be taken:

- Apply the appropriate patches or appropriate mitigations provided by GitLab to vulnerable systems immediately after appropriate testing.
- Upgrade software and operating systems, applications, and firmware on network assets in a timely manner for prevention.
- Use the right Vulnerability Management Tools to assess endpoint, networks or applications for known weaknesses.
- Apply the Principle of Least Privilege to all systems and services.
- Apply advanced application control and protection to enforce granular control over all application access, communications, and privilege elevation attempts.
- Kindly ensure that your Endpoint Security and Perimeter security products are updated with the latest signatures to detect these threats.

References

https://cybersecuritynews.com/cisa-gitlab-path-traversal/#google_vignette
https://thehackernews.com/2026/09/gitlab-cvss-10-file-read-flaw-draws-in.html
https://github.com/solivaquaant/CVE-2026-85706

CVE

CVE-2026-85706

Smarttech
YOUR 24/7 SECURITY PARTNER

www.smarttech247.com