DevOps platform GitLab recently released patches for seven vulnerabilities, including a high-severity flaw that allowed threat actors to take over people’s accounts.

As picked up by BleepingComputer, the highlight of the security advisory is an XSS weakness in the VS code editor (Web IDE), that threat actors can exploit via malicious pages. Although the attackers can abuse the flaw without authentication, the bug still requires victim interaction, making abusing the bug somewhat more complex.

The bug is tracked as CVE-2024-4835, and is currently waiting on a severity score.

Targeting GitLab users

"Today, we are releasing versions 17.0.1, 16.11.3, and 16.10.6 for GitLab Community Edition (CE) and Enterprise Edition (EE)," GitLab said. "These versions contain important bug and security fixes, and we strongly recommend that all GitLab installations be upgraded to one of these versions immediately."

Stealing people’s GitLab accounts could have major ramifications, BleepingComputer reports. For example, threat actors could use the accounts to inject malware into CI/CD (Continuous Integration/Continuous Deployment) environments, thus compromising the victim organization’s repositories.

As a result, GitLab accounts are generally considered a popular target among hackers. Earlier this month, CISA warned of a maximum-severity zero-click account hijacking flaw that hackers are abusing in the wild. This flaw is tracked as CVE-2023-7028, and was patched in January this year.

When CISA adds vulnerabilities to its Known Exploited Vulnerabilities (KEV) catalog, that usually means that threat actors can use it to target federal agencies. At time of writing, around 2,000 endpoints were still vulnerable to hackers.

Are you a pro? Subscribe to our newsletter

Sign up to the TechRadar Pro newsletter to get all the top news, opinion, features and guidance your business needs to succeed!

Besides the XSS weakness, the security advisory addresses six additional medium-severity flaws, including a Cross-Site Request Forgery (CSRF) via the Kubernetes Agent Server, a flaw tracked as CVE-2023-7045, and a denial-of-service vulnerability that threat actors can

abuse to prevent users from loading GitLab web resources. This vulnerability is tracked as CVE-2024-2874.