What we know so far about Red Hat's GitLab instance breach

By Berry Zwets

Published: 2025-10-03 · Archived: 2026-04-05 16:12:12 UTC

Red Hat is investigating a security incident involving a self-managed GitLab Community Edition instance used solely for Red Hat Consulting. On October 3, the company published a short blog post on the incident.

Red Hat says it acted immediately after detecting the compromise, the attacker lost access, the instance was isolated, and the incident was reported to the authorities. The investigation is ongoing.

Hackers calling themselves Crimson Collective claim to have stolen data from 28,000 internal Red Hat projects, totaling nearly 570 GB. BleepingComputer reports that data from about 800 Customer Engagement Reports was also taken. These reports can contain infrastructure details, configuration data, authentication keys, and other sensitive customer information. The hackers say the breach occurred about two weeks ago. On Telegram, they published a directory listing of stolen repositories and a list of customer reports from 2020 to 2025. The CER list includes organizations from various sectors, with names such as Bank of America, T-Mobile, AT&T, Fidelity, and Walmart.

At 5:30 PM CEST on October 2, Red Hat issued a correction to reporting we covered. We erroneously stated a GitHub environment was exposed, while instead the compromise revolved around a self-managed GitLab instance: “The security incident we are investigating and is related to a GitLab instance used solely for Red Hat Consulting on consulting engagements, not GitHub,” a spokesperson said. Red Hat has confirmed the incident relating to its GitLab instance, but declined to comment on specific claims about the repositories and customer reports. The company says there is no reason to believe the issue affects other Red Hat services or products and adds that it is very confident in the integrity of its software supply chain.

GitLab, which is not directly involved in the breach, also commented: “There has been no breach of GitLab’s managed systems or infrastructure. GitLab remains secure and unaffected.” GitLab added: “The incident refers to Red Hat’s self-managed instance of GitLab Community Edition, our free open-core offering. Customers who deploy free, self-managed instances on their own infrastructure are responsible for securing their instances, including applying security patches, configuring access controls, and maintenance.” GitLab encourages all self-managed customers to update to the latest version and follow security guidance available in its Handbook: https://about.gitlab.com/security/hardening/

What the attackers claim

Crimson Collective says it found authentication keys, full database URIs, and other private information inside Red Hat code and CERs, and used these to access downstream customer infrastructure. The group says it attempted to contact Red Hat with extortion demands but received only a standard response to submit a vulnerability report to the security team. According to the hackers, the ticket they created was repeatedly forwarded to various people, including employees in Red Hat’s legal and security departments.

The same group also claimed responsibility for briefly vandalizing Nintendo's topic page last week. Red Hat has not responded to further questions and continues to state that the security and integrity of systems and entrusted data are its highest priority.

Also read: Google refutes reports of major Gmail breach
