Cybercrime group claims to have breached Red Hat 's private GitHub repositories

By Pierluigi Paganini

Published: 2025-10-02 · Archived: 2026-04-05 16:56:35 UTC

The cybercrime group calling itself the Crimson Collective claimed to have compromised Red Hat ‘s private GitHub repositories.

The Crimson Collective claimed it had stolen 570GB from Red Hat ’s private GitHub repositories, including 28,000 projects and approximately 800 Customer Engagement Reports (CERs) with sensitive network data. CERs often contain sensitive info, including infrastructure details, configurations, and tokens that attackers could exploit to target customers’ networks.

The U.S.-based multinational software company confirmed the data breach, but did not verify Crimson Collective.

On September 24, 2025, the threat actors shared on a Telegram channel a full file tree, CER list, and screenshots as proof of the security breach.

“Btw gained access to some of their client’s infrastructure as well, already warned them but yeah they preferred ignoring us,” the Crimson Collective wrote on Telegram.

The file tree includes thousands of repositories referencing major banks, telecoms, airlines, and public-sector organizations, such as Citi, Verizon, Siemens, Bosch, JPMC, HSBC, Merrick Bank, Telstra, Telefonica, and even mentions the U.S. Senate.

The threat actor also shared evidence of their attempt to contact RedHat.

Red Hat said protecting systems and data is a top priority, adding the incident doesn’t affect its other services or products, and its supply chain remains secure.

“Red Hat is aware of reports regarding a security incident related to our consulting business and we have initiated necessary remediation steps,” Red Hat told BleepingComputer.

“The security and integrity of our systems and the data entrusted to us are our highest priority. At this time, we have no reason to believe the security issue impacts any of our other Red Hat services or products and are highly confident in the integrity of our software supply chain.”

Follow me on Twitter: @securityaffairs and Facebook and Mastodon

Pierluigi Paganini

(SecurityAffairs – hacking, data breach)
