Red Hat Data Breach - Threat Actors Claim Breach of 28K Private GitHub Repositories

By Guru Baran

Published: 2025-10-02 · Archived: 2026-04-05 15:09:19 UTC

An extortion group known as the Crimson Collective claims to have breached Red Hat's private GitHub repositories, making off with nearly 570GB of compressed data from 28,000 internal repositories.

This data theft is being regarded as one of the most significant breaches in technology history, involving the unauthorized extraction of source code and sensitive confidential information.

The stolen repositories allegedly reference thousands of organizations across multiple industries, including major banks, telecoms, airlines, and public-sector institutions.

Notable names mentioned within the reportedly compromised repository tree include Citi, Verizon, Siemens, Bosch, JPMC, HSBC, Merrick Bank, Telstra, Telefonica, and even the U.S. Senate.

The range of referenced clients underscores the potential scale and downstream risk for critical supply chains worldwide if the breach claims are accurate.

Sensitive Credentials and Configuration Data Exposed

What makes the Crimson Collective's allegations especially alarming is the nature of the leaked content.

Initial reviews suggest that the stolen data includes a substantial trove of credentials, CI/CD secrets, pipeline configuration files, VPN connection profiles, infrastructure blueprints, inventories, Ansible playbooks, OpenShift deployment guides, CI/CD runner instructions, container registry configurations, Vault integration secrets, backup files, and exported GitHub/GitLab configuration templates.

The leak's inventory reveals both operational and architectural information that adversaries could exploit for secondary infiltrations or extortion attempts.

Security professionals warn that exposed credentials and infrastructure details can rapidly escalate from technical nuisance to existential business risk, especially for organizations relying heavily on automated DevOps and Infrastructure-as-Code (IaC) paradigms.

Red Hat is not alone in facing the risk of credentials or config files appearing in unexpected code repositories.

Recent security research has highlighted the perils of Shadow IT, where personal or side project repositories by employees accidentally expose sensitive enterprise secrets, sometimes granting privileged access to internal corporate containers or cloud infrastructure.

Such exposure can lead to systemic risks beyond the original organization, impacting downstream users and partners.

This breach appears to be a potent illustration of multi-level supply-chain risk: attack paths may traverse CI/CD systems, container registries (such as Quay), automation playbooks, and public/private configuration backups, multiplying impact vectors for both Red Hat and its customers.

Red Hat has not yet made a public statement confirming or denying any connections to its own infrastructure. Cybersecurity News reached out to Red Hat to find more details on the developing story.

The Crimson Collective's claims and their potential for industry-wide ripple effects continue to unfold. All eyes remain on Red Hat, its customers, and the global supply chain as investigators race to contain what may be one of the broadest source code exposures on record.

Follow us on Google News, LinkedIn, and X for daily cybersecurity updates. Contact us to feature your stories.

Source: https://cybersecuritynews.com/red-hat-data-breach/