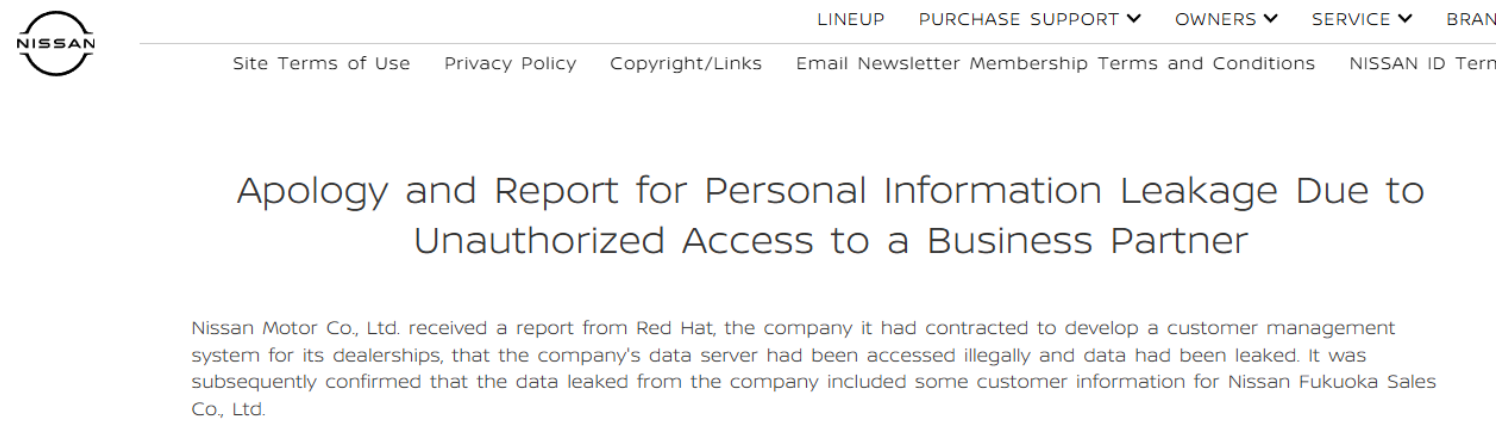
# 2025/12/25

# Another Breach for Nissan: 21,000 Customer Records Leaked After Red Hat Server Hack

Article By : Dipanshu Kumar (Threat Ledger)

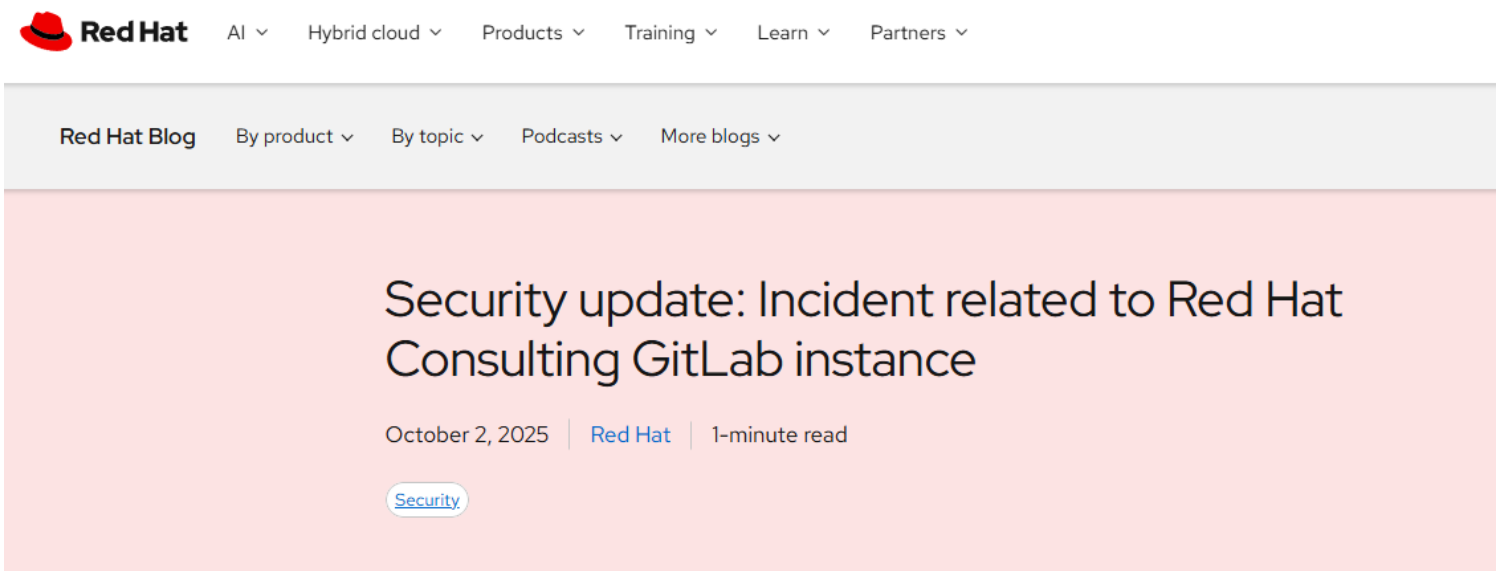
So Nissan Confirms Data Exposure of 21,000 Customers After Red Hat Security Breach.




Url : https://www3.nissan.co.jp/siteinfo/information_251205.html

Nissan Motor Co., Ltd. has confirmed that the personal data of approximately **21,000 customers in Japan** was exposed following a cybersecurity incident at **Red Hat**, a U.S.-based software company contracted to support Nissan's customer management systems.

The breach did not originate within Nissan's own infrastructure. Instead, attackers gained unauthorized access to a **Red Hat–managed GitLab environment**, highlighting once again how third-party systems can become critical weak points in modern digital supply chains.




https://www.redhat.com/en/blog/security-update-incident-related-red-hat-consulting-gitlab-instance

# What We Know So Far

According to Nissan, Red Hat detected suspicious activity on **September 26, 2025**, and informed the automaker on **October 3**. Nissan says it immediately reported the incident to Japan's **Personal Information Protection Commission** and began notifying affected customers.
The leaked data belongs to customers of **Nissan Fukuoka Sales Co., Ltd.**, a regional sales company serving customers who purchased vehicles or received maintenance services in the Fukuoka area.
The exposed information includes:

- Full names
- Physical addresses
- Phone numbers
- Email addresses (some partial)
- Internal customer data used for sales operations

Nissan emphasized that **no financial or payment information**, including credit card details, was involved. At this stage, the company says there is **no evidence the leaked data has been misused**, but customers have been advised to stay alert for suspicious phone calls, emails, or mail that could indicate phishing or fraud attempts.

**Kevin Beaumont**
@GossiTheDog@cyberplace.social

Crimson Collective are trying to extort Redhat

They've stolen about ~1tb of data related to corporate customers. File list:

archive.ph/0MwqJ

Since RedHat doesn't want to answer to us.

Hide

- Over 28000 repositories were exported, it includes all their customer's CERs and analysis of their infra' + their other dev's private repositories, this one will be fun.

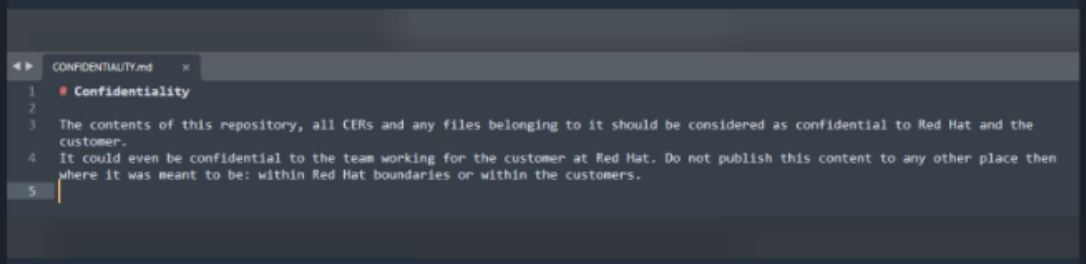
We have given them too much time already to answer lol instead of just starting a discussion they kept ignoring the emails so yeah alright brodie.

(Screenshots only show the consulting / customer-success part, have more than that)

❤️ 3 🔥 1 1

268 miku, 15:06

Crimson Collective




this is actually so funny

😁 3

277 miku, 15:06

Crimson Collective

Btw gained access to some of their client's infrastructure as well, already warned them but yeah they preferred ignoring us

🥰 2 🤯 1

279 miku, 15:07

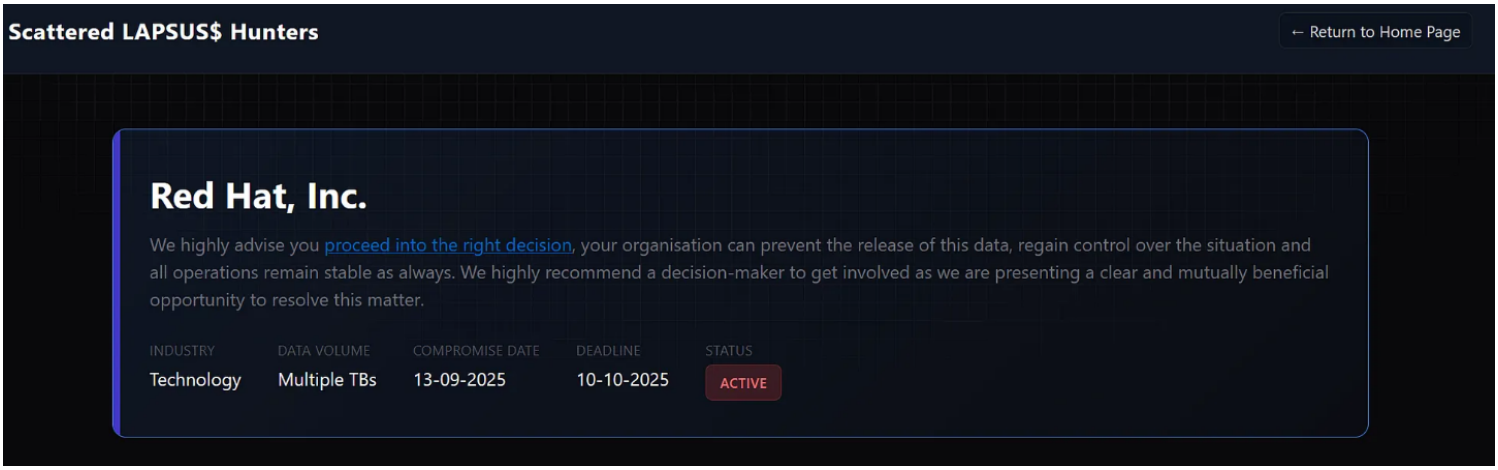
#threatintel

Oct 02, 2025, 10:35 AM · · Web

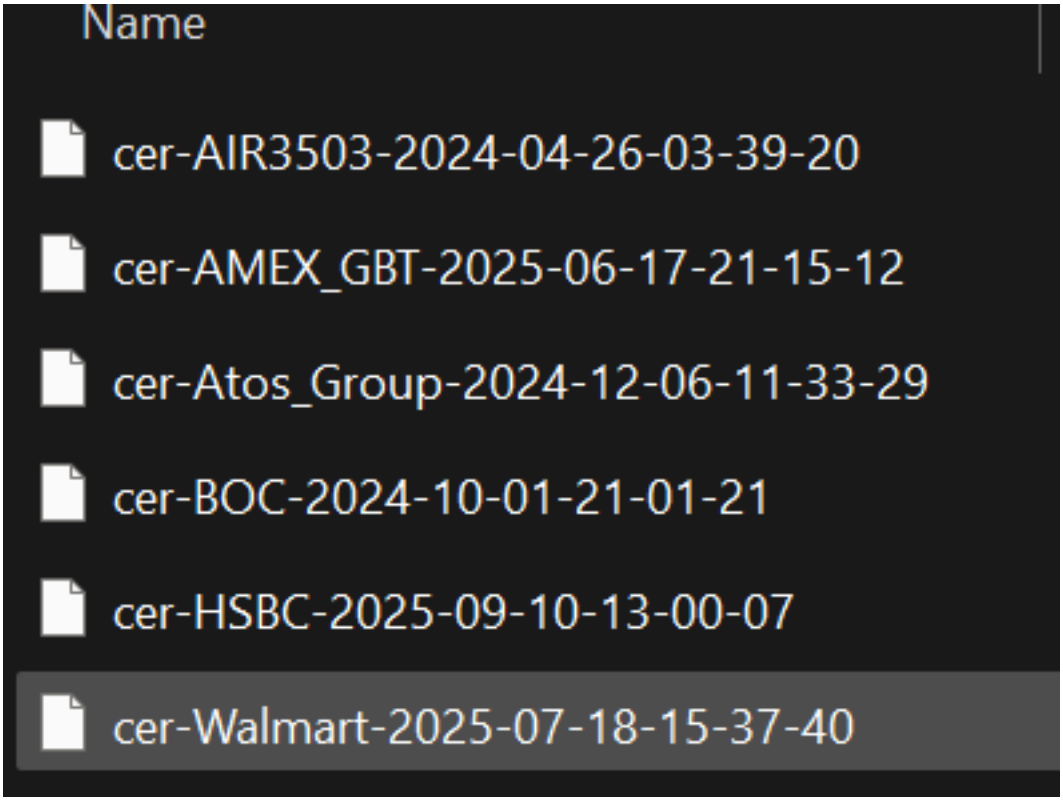
# Inside the Red Hat Breach

The incident at Red Hat became public in early October, when the company acknowledged that an unauthorized third party had accessed and copied data from a **self-managed GitLab instance** used by its consulting division.

Threat actors operating under the name **Crimson Collective** claimed responsibility for the attack, stating they had exfiltrated **hundreds of gigabytes of compressed data** from around **28,000 private repositories**. The group later published file trees and screenshots as proof of access.




Shortly after, the well-known hacking group **ShinyHunters** escalated pressure by hosting samples of the stolen data on its extortion platform.




Security researchers noted that the breach potentially placed **thousands of high-profile organizations** at risk, as Red Hat's repositories reportedly referenced banks, airlines, telecom providers, and public-sector entities worldwide. Red Hat has said it removed the attackers' access, isolated the affected systems, and launched an

ongoing investigation, while stressing that its broader services and supply chain were not impacted.


To stay updated with the latest cybersecurity and data breach news, along with practical learning resources, courses, and free materials, follow me on LinkedIn. You can also explore and follow the open-source GitHub repository **ThreatLedger** for curated threat intelligence, breach insights, and security research shared with the community.