Fashion giant Chanel hit in wave of Salesforce data theft attacks

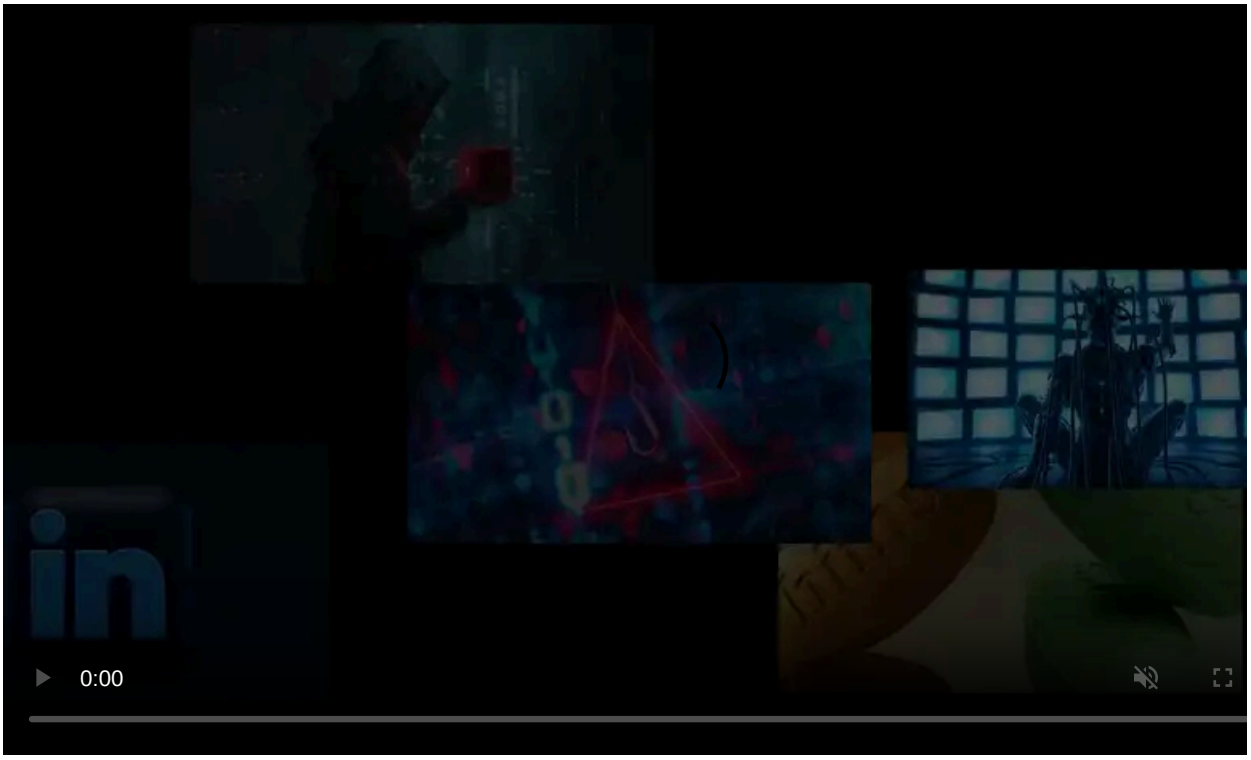
By Lawrence Abrams

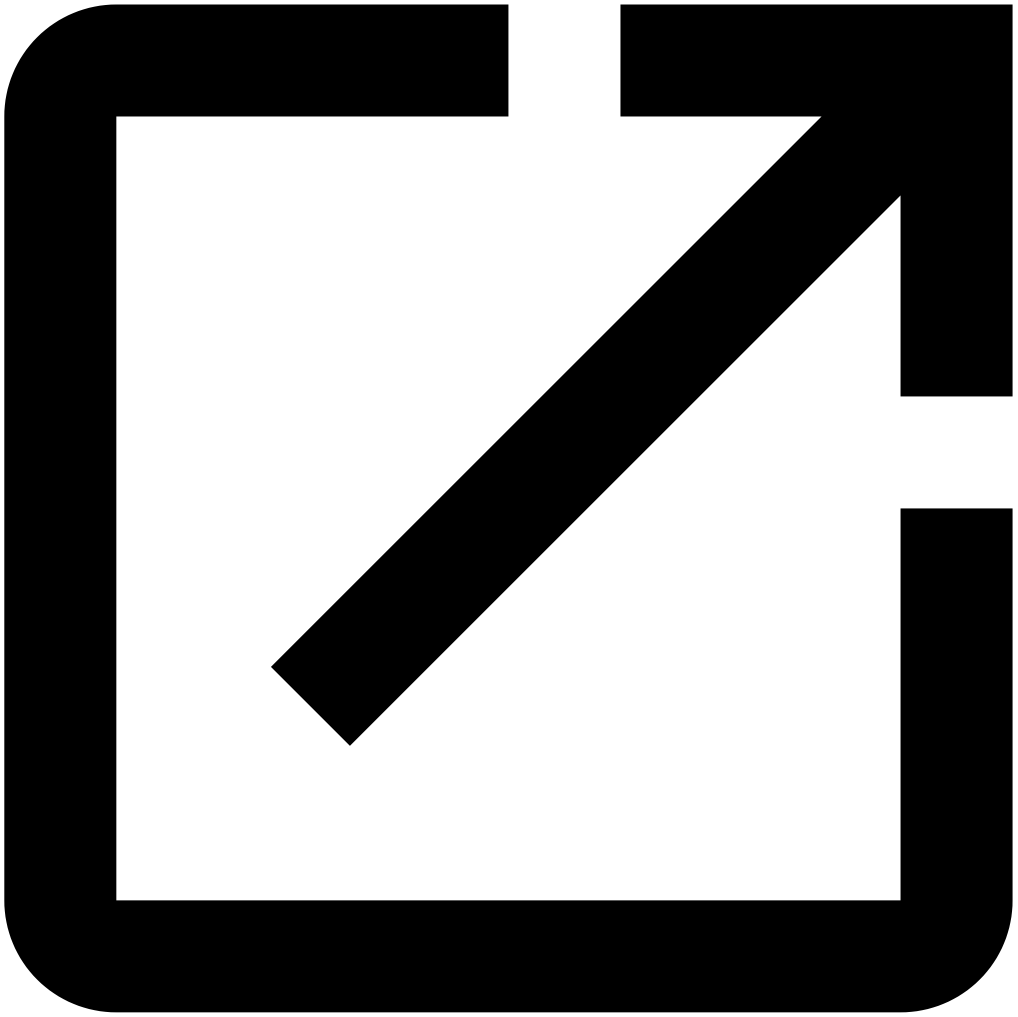
Published: 2025-08-04 · Archived: 2026-04-05 18:46:10 UTC

French fashion giant Chanel is the latest company to suffer a data breach in an ongoing wave of Salesforce data theft attacks.

Chanel says the breach was first detected on July 25th after threat actors gained access to a Chanel database hosted at a third-party service provider, as first reported by WWD.

The breach only impacted customers in the United States and exposed personal contact information.


0:00



"Based on the findings of the investigation, the data obtained by the unauthorized external party contained limited details of a subset of individuals who contacted our client care center in the U.S. —specifically name, email address, mailing address and phone number," a Spokesperson told WWD.

"No other information was contained in the database. The clients affected have been informed."

While Chanel has not replied to our emails and the name of the third-party service provider was not mentioned, BleepingComputer has learned that it was stolen from the company's Salesforce instance.

This attack has been attributed to the ongoing wave of Salesforce data-theft attacks conducted by the ShinyHunters extortion group.

As first reported by Mandiant, threat actors have been actively targeting Salesforce customers in vishing (voice phishing) attacks to compromise credentials or to trick employees into authorizing a malicious OAuth app with their organization's Salesforce portal.

Once they gain access to the Salesforce instance, they exfiltrate the database and use it as leverage in extortion demands on customers.

In a statement to BleepingComputer, Salesforce emphasized that its platform was not compromised, but rather, customers' accounts are being breached in social engineering attacks.

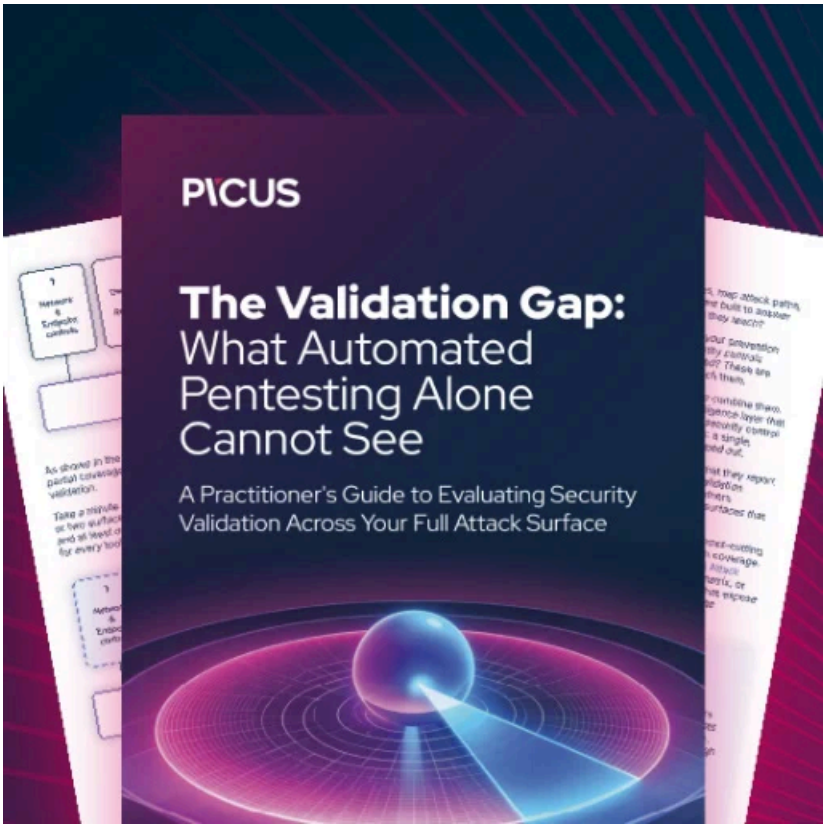
"Salesforce has not been compromised, and the issues described are not due to any known vulnerability in our platform. While Salesforce builds enterprise-grade security into everything we do, customers also play a critical role in keeping their data safe — especially amid a rise in sophisticated phishing and social engineering attacks," Salesforce told BleepingComputer.

"We continue to encourage all customers to follow security best practices, including enabling multi-factor authentication (MFA), enforcing the principle of least privilege, and carefully managing connected applications. For more information, please visit: https://www.salesforce.com/blog/protect-against-social-engineering/."

The threat actors have not publicly leaked the data for any companies to date, with companies currently extorted via email.

Other companies impacted in these Salesforce data theft attacks include Adidas, Qantas, Allianz Life, and the LVMH brands, Louis Vuitton, Dior, and Tiffany & Co.

BleepingComputer knows of other allegedly breached companies that have not yet disclosed attacks, but we have not been able to verify them independently as of yet.



Automated Pentesting Covers Only 1 of 6 Surfaces.

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

Source: https://www.bleepingcomputer.com/news/security/fashion-giant-chanel-hit-in-wave-of-salesforce-data-theft-attacks/