Cisco Data Breach May Tie to ShinyHunters Salesforce Campaign

TL;DR

Cisco has disclosed a data breach involving a third-party cloud CRM system accessed through a voice phishing attack. While Salesforce hasn't been confirmed, the method mirrors the ShinyHunters campaign that previously hit Qantas, Allianz Life, Chanel, and LVMH.

The attacker accessed Cisco.com user data, including names, emails, and phone numbers. No sensitive or internal information was stolen. Aspire is monitoring the situation and advises organizations to follow the same recommendations from our original Emergency Flash Notice.

Overview

Aspire's CTI team is monitoring a newly disclosed data breach at Cisco that may be connected to the same vishing campaign outlined in our previous flash notice regarding ShinyHunters. While not yet confirmed, overlaps suggest the same threat actor and tactic could be involved.

According to Cisco, the attacker gained access to a third-party cloud-based CRM system via voice phishing targeting a Cisco employee. The threat actors stole basic user profile data from Cisco.com account holders, including names, email addresses, phone numbers, and metadata. Cisco has not confirmed whether Salesforce was the impacted CRM platform, but the method of access mirrors those used in the ShinyHunters campaign previously impacting Qantas, Allianz Life, LVMH, Adidas, and others.

This breach occurred on July 24, 2025, aligning with the timeline of the Salesforce campaign. No passwords or confidential organizational data were stolen, and there has been no confirmed ransom demand or data leak.

Customers should continue auditing connected apps and enforcing strong, phishing-resistant MFA. We will issue another update if attribution to ShinyHunters is confirmed or if any indicators of compromise become available. Until attribution is confirmed, we advise organizations to follow the same security recommendations provided in the original Emergency Flash Notice.

Aspire Protects

- ShinyHunters is exploiting human trust via social engineering. Here is a quick recap of how they are doing it:
    - They call employees pretending to be IT support (vishing).
    - They direct them to the connected app setup page in Salesforce.
    - The victim is asked to enter a malicious connection code.
    - That code authorizes a rogue app, giving attackers persistent access without needing to hack Salesforce itself.
- To stay safe, Aspire recommends the following:
    - Train users to verify any IT requests received over the phone. No IT team should ever ask for app authorization codes.
    - Mandate phishing-resistant MFA, such as hardware security keys (FIDO2/U2F) or platform authenticators.
        - Avoid relying solely on push-based MFA or SMS codes, which can be phished or socially engineered.
- Audit all connected apps in Salesforce immediately and remove unrecognized or suspicious entries.
- Enforce IP restrictions on Salesforce login and app connections.
- Enable Salesforce Shield for anomaly detection, data loss prevention, and audit trail logging

TTPs to Watch

Initial Access

- Phishing [T1566.001] – Spoofed Okta login pages used to capture credentials.
- Vishing [T1598.004] – Threat actors call employees pretending to be internal IT, instructing them to authorize malicious OAuth apps.

Persistence

- Abuse of OAuth Tokens [T1528] – Linked apps maintain access beyond password resets.

Collection

- Data from Information Repositories [T1213] – Exfiltration of Salesforce “Accounts” and “Contacts” data tables.

Command and Control

- Web Service [T1102] – Data transfer likely occurs via compromised app infrastructure.

IoCs

Email

- shinycorp@tuta[.]com
- shinygroup@tuta[.]com

Proxy infrastructure patterns

- Use of Mullvad VPN IP addresses and TOR exit nodes during social engineering phone calls and data exfiltration windows.

Targeted Industries

ShinyHunters is stealing customer data from Salesforce environments across industries like:

- Aviation
- Insurance
- Retail
- Technology

Aspire’s Service Offerings

- **Aspire Managed XDR (MXDR)**
    - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security

professionals to identify and respond to threats across a broader attack surface.
    - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors.
    - Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyber attacks.
- **Aspire Incident Response**
    - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.
    - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

Supporting Documentation

Extortion Campaign by ShinyHunters Targets AWS - LevelBlue - Open Threat Exchange

Hackers abuse malicious version of Salesforce tool for data theft, extortion | Cybersecurity Dive

Cisco discloses data breach impacting Cisco.com user accounts

Cisco Event Response: Vishing Attack Impacting Third-Party CRM System