Cisco Impacted by Trivy Supply Chain Attack While Facing Separate ShinyHunters Data Theft Claims

TL;DR

A malicious version of Trivy (v0.69.4) was pushed through a compromised GitHub build process, allowing an infostealer to run in CI/CD pipelines and on developer machines. Stolen credentials from this campaign were later used to access Cisco's internal development environment, leading to repository access and AWS activity.

At the same time, the threat actor group ShinyHunters claims it has stolen over 3 million Salesforce records and other internal data from Cisco, though those claims are not fully confirmed. Organizations should treat the Trivy exposure as active risk and monitor for follow-on activity tied to either incident.

Overview – Cisco and Trivy Supply Chain Attack

There is a supply chain attack involving Trivy (v0.69.4) where threat actors pushed a malicious update through its GitHub build pipeline. The update included an infostealer that runs in CI/CD pipelines and on developer machines.

The malware searches memory and local files for credentials. It grabs cloud keys, SSH keys, API tokens, and environment variables, then sends them to attacker-controlled servers. This activity directly impacted Cisco. Threat actors used stolen credentials from this campaign to access Cisco's development environment. They cloned repositories and used AWS keys for unauthorized activity.

This isn't tied to a CVE. The tool itself was compromised. If it ran in your environment, an attacker could have access to your build systems and data.

Overview – Cisco and ShinyHunters Claims

Cisco is also dealing with a separate situation involving the threat actor group ShinyHunters, known for data theft and extortion.

The group claims it has stolen over 3 million Salesforce records, along with GitHub repositories, AWS data, and other internal corporate information. The data is believed to include personally identifiable information (PII) and internal cloud assets. The group is attempting to extort Cisco and has set a deadline (April 3, 2026) for payment.

These claims haven't been confirmed, but screenshots show access to AWS storage and internal systems. The reported access may be tied to multiple entry points,

including previously disclosed voice phishing activity and potential cloud account compromise.

There is no confirmed CVE tied to this activity. If the claims are true, exposed customer and internal data could be used for fraud, phishing, or follow-on attacks against organizations connected to Cisco.

What This Means for You

These are two separate incidents, but both involve unauthorized access. One is tied to a compromised tool, and the other may involve stolen data and extortion. Both should be treated as active risk until more is confirmed. Aspire Technology Partners is actively monitoring this activity and will notify customers if any related threats are observed in their environments. For more details on how we can help protect your organization, contact Aspire's Customer Success Management team.

Aspire Protects

- Supply Chain Attack
  - Rotate all credentials tied to CI/CD pipelines, cloud platforms, and developer systems.
  - Stop using Trivy v0.69.4 and review recent workflow activity.
  - Audit GitHub Actions for unauthorized changes or external calls.
  - Review logs for unusual repository access or cloud activity.
  - Monitor for connections to known malicious domains.
  - Reimage systems if compromise is suspected.
- ShinyHunters Incident
  - Review Salesforce, AWS, and GitHub access logs for unusual activity.
  - Reset credentials tied to cloud platforms and CRM systems.
  - Monitor for signs of data exposure or unauthorized data access.
  - Prepare for potential phishing or fraud campaigns targeting users or customers.
  - Validate whether any internal or customer data has been accessed or exfiltrated.

TTPs to Watch

Trivy/Cisco Supply Chain Attack

Credential Access

- Unsecured Credentials [T1552] – The attacker may search local files and configuration paths to collect stored credentials.

Credential Access

- OS Credential Dumping [T1003] – The attacker may access process memory to extract sensitive authentication data.

Collection

- Data from Local System [T1005] – The attacker may gather sensitive files from developer systems and CI/CD environments.

Exfiltration

- Exfiltration Over C2 Channel [T1041] – The attacker may transmit stolen data to external infrastructure.

Persistence

- Create or Modify System Process [T1543] – The attacker may create a system service to maintain access on compromised systems.

Cisco/ShinyHunters

Initial Access

- Phishing [T1566] – The attacker may use voice phishing or social engineering to gain access to accounts.

Credential Access

- Valid Accounts [T1078] – The attacker may use legitimate credentials to access cloud and CRM systems.

Collection

- Data from Cloud Storage Object [T1530] – The attacker may access data stored in cloud environments such as AWS S3 or CRM platforms.

Exfiltration

- Exfiltration Over Web Service [T1567] – The attacker may transfer stolen data using web-based services or cloud platforms.

IoCs

Trivy/Cisco Supply Chain Attack

Domains

- scan[.]aquasecurtiy[.]org
- can[.]aquasecurtiy[.]org
- tdtqy-oyaaa-aaaae-af2dq-cai[.]raw[.]icp0[.]io

Files

- tpcp.tar.gz
- ~/.config/systemd/user/sysmon.py

Behavioral

- GitHub Actions pulling unexpected external files
- Unauthorized repository creation within GitHub accounts
- Credential access activity from CI/CD runner processes
- Outbound traffic from build systems to unknown domains

Cisco/ShinyHunters

Behavioral IoCs

- Unusual access to Salesforce data or bulk record exports
- Unexpected AWS S3 bucket or EC2 volume access
- Large-scale data access or transfer activity
- Suspicious login activity tied to cloud or CRM platforms

(No confirmed domains or malware artifacts have been released at this time.)

Targeted Industries

The Trivy supply chain attack impacts organizations that rely on developer tools, CI/CD pipelines, and cloud environments.

- Education
- Energy
- Finance
- Healthcare
- Legal
- Manufacturing
- Public Sector
- Retail

Aspire 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

https://github.com/aquasecurity/trivy/ - Malicious Git Repository

Cisco threatened by ShinyHunters after alleged data heist | Cybernews

Trivy Security incident 2026-03-19 conclusion · aquasecurity/trivy · Discussion #10462 · GitHub

Trivy Supply Chain Attack: GitHub Actions Compromise - Upwind

Trivy Security incident 2026-03-19 · aquasecurity/trivy · Discussion #10425 · GitHub

Aqua Security Trivy GitHub Action Compromised - NHS England Digital