

China-Nexus Threat Group ‘Velvet Ant’ Exploits Cisco Zero-Day (CVE-2024-20399) to Compromise Nexus Switch Devices – Advisory for Mitigation and Response

By Sygnia

Published: 2024-07-01 · Archived: 2026-04-05 15:08:41 UTC

Learn about the forensic investigation by Sygnia, the cyber espionage operation by Velvet Ant, and best practices for safeguarding your network against sophisticated threats.

Overview

- On July 1, Cisco [published](#) an advisory regarding CVE-2024-20399, a newly discovered command injection vulnerability in the Cisco NX-OS Software CLI. This vulnerability affects a wide range of Cisco Nexus devices.
- Sygnia discovered and reported this vulnerability to Cisco and provided detailed information about the exploit and the subsequent attack flow.
- The vulnerability was identified as part of a larger forensic investigation performed by Sygnia of a China-nexus cyber espionage operation that was conducted by a threat actor Sygnia dubs as ‘Velvet Ant’.
- Following Velvet Ant’s exploitation of CVE-2024-20399, the group successfully executed malicious code on the underlying Linux OS of the Nexus switch.
- Network appliances, particularly switches, are often not monitored, and their logs are frequently not forwarded to a centralized logging system. This lack of monitoring creates significant challenges in identifying and investigating malicious activities.
- Consistently applying and adhering to security best practices ensures resilient defense mechanisms, effectively safeguarding against sophisticated threats, including state sponsored attacks, such Velvet Ant.

Introduction

Background

Cisco NX-OS Software is a network operating system specifically used for Cisco’s Nexus series of switches. Although NX-OS is based on a Linux kernel, it abstracts away the underlying Linux environment and provides its own set of commands using the NX-OS CLI. In order to execute commands on the underlying Linux operating system from the Switch management console, an attacker would need a “jailbreak” type of vulnerability to escape the NX-OS CLI context.

CVE-2024-20399 that was identified by Sygnia allows an attacker with valid administrator credentials to the Switch management console to escape the NX-OS CLI and execute arbitrary commands on the Linux underlying operating system.

Sygnia identified that CVE-2024-20399 was exploited in the wild by a China-nexus threat group as a ‘zero-day’ and shared the details of the vulnerability with Cisco. By exploiting this vulnerability, a threat group – dubbed ‘Velvet Ant’ – successfully executed commands on the underlying operating system of Cisco Nexus devices. This exploitation led to the execution of a previously unknown custom malware that allowed the threat group to remotely connect to compromised Cisco Nexus devices, upload additional files, and execute code on the devices.

Relevance and Impact for Your Organization

Cisco Nexus switches are prevalent in enterprise environments, especially within data centers. Exploiting the identified vulnerability requires the threat group to possess valid administrator-level credentials and have network access to the Nexus switch. Given that most Nexus switches are not directly exposed to the internet, a threat group must first achieve initial access to the organization’s internal network to exploit this vulnerability. Consequently, the overall risk to organizations is reduced by the inherent difficulty in obtaining the necessary access.

Despite the substantial pre-requisites for exploiting the discussed vulnerability, this incident demonstrates the tendency of sophisticated threat groups to leverage network appliances – which are often not sufficiently protected and monitored – to maintain persistent network access; the incident also underscores the critical importance of adhering to security best practices as a mitigation against this type of threat. The recommended mitigation strategies are detailed in the Hardening and Prevention section below.

What You Should Do

General Details and Affected Products

The vulnerability has CVE ID CVE-2024-20399, and a CVSS score of 6.0 (medium severity).

As of version 1.0 of Cisco’s advisory regarding the CVE, the following products are affected:

- MDS 9000 Series Multilayer Switches (CSCwj97007) *
- Nexus 3000 Series Switches (CSCwj97009)
- Nexus 5500 Platform Switches (CSCwj97011)
- Nexus 5600 Platform Switches (CSCwj97011)
- Nexus 6000 Series Switches (CSCwj97011)
- Nexus 7000 Series Switches (CSCwj94682) *
- Nexus 9000 Series Switches in standalone NX-OS mode (CSCwj97009) *

* See the detailed list of affected products in Cisco’s [advisory](#).

Patching

Cisco has released software updates that address the vulnerability described in this advisory. Updating the systems of affected devices is the primary mitigation strategy for licensed devices. For cases in which software updates are not available, this incident demonstrates the critical importance of adopting security best practices to prevent access to devices in the first place.

Hardening and Prevention

The prevention and hardening strategies outlined below are designed to provide organizations with robust measures to counter threats related to unauthorized access and command execution vulnerabilities in network equipment such as CVE-2024-20399.

- 1. Restrict administrative access:** Utilize a Privileged Access Management (PAM) solution or a dedicated, hardened, jump server with multi-factor authentication (MFA) enforced, to restrict access to network equipment. If these options are not feasible, restrict access to specific network addresses, such as an Out-Of-Band (OOB) network. Implementing a secure point for management access significantly limits a threat groups' ability to gain access to switches and other network equipment without being detected.
- 2. Use central authentication, authorization, and accounting management for users (AAA):** Utilizing TACACS+ and systems such as Cisco ISE can help streamline and enhance security, especially in environments with numerous switches. Centralized user management ensures that local user accounts are not scattered across individual switches, and simplifies monitoring, password rotation, and access reviews. Additionally, in the event of a compromise, centralized management allows for quick and efficient user remediation across all network equipment.
- 3. Enforce a strong password policy and maintain good password hygiene:** Although passwords should not be the sole security measure, ensuring that administrative users have complex, securely stored passwords is crucial. Preferably, use a Privileged Identity Management (PIM) solution that can auto-rotate administrative account passwords, or a password vault with restricted access. Avoid storing passwords in unsecured locations, such as Excel spreadsheets or shared folders.
- 4. Restrict outbound internet access for devices:** Restrict switches from initiating outbound connections to the internet to reduce the risk of them being exploited by external threats, or used to communicate with malicious actors. Implement strict firewall rules and access control lists (ACLs) to ensure that only necessary traffic is allowed, further enhancing the security of your network infrastructure.
- 5. Implement regular patch management and vulnerability management practices:** Regularly review and apply patches to all network devices to address newly discovered vulnerabilities such as CVE-2024-20399 to reduce the risk of exploitation. Utilize automated tools such as vulnerability scanners to identify and prioritize existing vulnerabilities in network equipment.

Monitoring and Detection

Network equipment, especially switches, often lacks adequate monitoring by organizations. Enhancing visibility and forwarding logs to a central logging solution are crucial first steps in identifying malicious activities on network devices. To monitor for exploitation attempts, consider the following actions:

- 1. Enable Syslog on All Switches:** Ensure that all network switches are configured to send log data to a centralized Syslog server.
 1. Cisco supports configuring different logging levels for specific modules.
 2. By default, Cisco switches only log failed authentication attempts. Consider changing the AUTHPRIV level to 6 to also include successful authentication attempts.
- 2. Set Up SIEM Integration:** Integrate switch logs with a Security Information and Event Management (SIEM) system to correlate events and detect anomalies.
- 3. Configure Alerts:** Utilize syslog information to establish alerts that help identify suspicious activities. For instance, set up alerts for SSH connections that do not originate from an authorized jump host, and for SSH

connections originating from network equipment.

4. **Set up Network Monitoring:** Regularly analyze network traffic to identify anomalous patterns associated with Cisco switches, with a focus on traffic involving management ports such as SSH and Telnet.
5. **Conduct Periodic Threat Hunts:** Design threat hunts focused on network devices.
 1. Exploitation of CVE-2024-20399 can be identified by analyzing commands executed on the device and searching for anomalies; such commands may include the output of the ‘show accounting log’ command.
 2. To identify a compromised switch running the malware deployed by Velvet Ant, analyze the output of ‘show sockets connection’, and search for processes listening on high ports.
 3. Note that to validate if a switch that exhibits suspicious indicators is indeed compromised, access to the underlying Linux operating system is required.
6. **Monitor Velvet Ant’s IOCs and TTPs:** Sygnia recently published a detailed [blog post](#) on the group, providing additional insights into their methods. Use the information in the blog to enhance detection capabilities, and to detect whether the threat group is present or active within your network.

Appendices

References

Cisco Advisory: <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP>

Sygnia’s blog on Velvet Ant:

<https://www.sygnia.co/blog/china-nexus-threat-group-velvet-ant/>

How Sygnia Can Help

Sygnia offers focused threat hunts and incident response services to navigate the challenges posed by CVE-2024-20399. Our experts are ready to assist in swiftly securing your environment against this and all vulnerabilities.

If you were impacted by this attack or are seeking guidance on how to prevent similar attacks, please contact us at contact@sygnia.co or our 24-hour hotline +1-877-686-8680.

This advisory and any information or recommendation contained here has been prepared for general informational purposes and is not intended to be used as a substitute for professional consultation on facts and circumstances specific to any entity. While we have made attempts to ensure the information contained herein has been obtained from reliable sources and to perform rigorous analysis, this advisory is based on initial rapid study, and needs to be treated accordingly. Sygnia is not responsible for any errors or omissions, or for the results obtained from the use of this Advisory. This advisory is provided on an as-is basis, and without warranties of any kind.

Source: <https://www.sygnia.co/threat-reports-and-advisories/china-nexus-threat-group-velvet-ant-exploits-cisco-0-day/>