ORDR SECURITY BULLETIN

ConnectWise Screenconnect CVEs

Background

ConnectWise ScreenConnect software is a comprehensive remote desktop and access software solution that provides secure, flexible, and efficient support across various industries and needs. It is part of ConnectWise's suite of products aimed at enhancing IT service delivery and support capabilities. ConnectWise ScreenConnect is commonly used by managed service providers (MSPs) to gain remote access to customer endpoints for services such as IT support.

The ConnectWise advisory indicated that in all versions of ScreenConnect prior to 23.9.8, there were two vulnerabilities.

Vulnerability Details

	CVE-2024-1709	CVE-2024-1708
Severity	**Critical** CVSS: 10	**High** CVSS: 8.4
Products Affected	ConnectWise ScreenConnect Software	ConnectWise ScreenConnect Software
Versions Affected	**Up to (excluding) 23.9.8**	**Up to (excluding) 23.9.8**
Details	Authentication bypass using an alternate path or channel to gain unauthorized access to confidential information or critical systems.	Improper limitation of a pathname to a restricted directory ("path traversal") via a Zip Slip attack.
Exploitability Score	**3.9**	**1.7**
Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H	CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:H/I:H/A:H
Impact Score	**6.0**	**6.0**
NVD Published Date	**02/21/2024**	**02/21/2024**
NVD Last Modified	**02/22/2024**	**02/22/2024**
Reference	https://nvd.nist.gov/vuln/detail/CVE-2024-1709	https://nvd.nist.gov/vuln/detail/CVE-2024-1708

Has This Been Exploited?

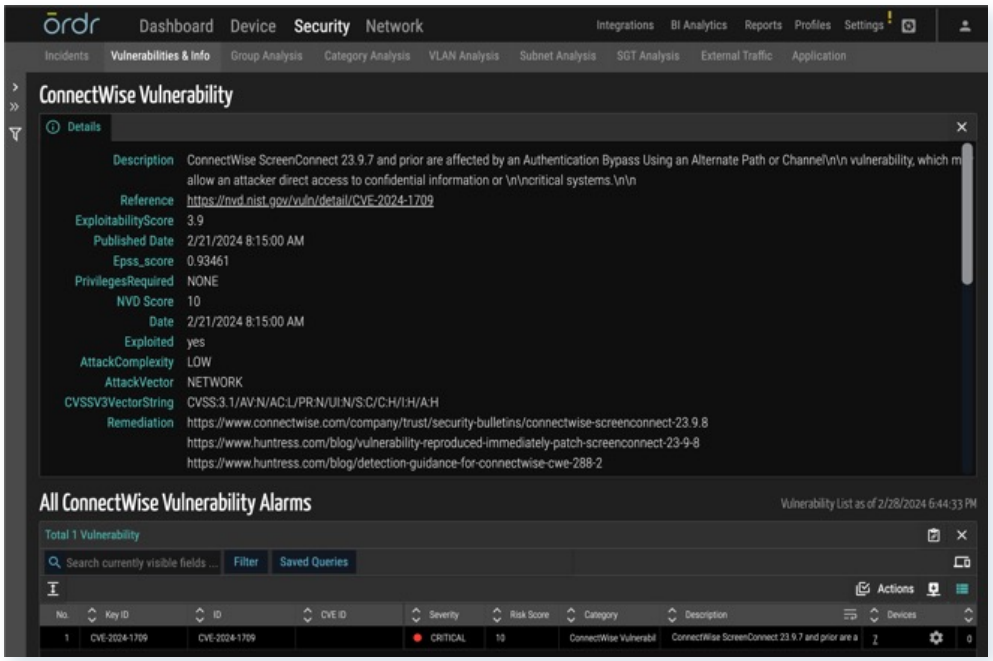
Yes, CVE-2024-1708 and CVE-2024-1709 have been exploited. These have been added to the Known Exploited Vulnerabilities Catalog by CISA due to evidence of active exploitation. Trend Micro says that more cybercrime groups, including the Black Basta and Bl00dy ransomware groups, have started exploiting the flaws.

Federal Civilian Executive Branch agencies must address vulnerabilities identified in this catalog by a specified due date, which for CVE-2024-1709 is Feb 29, 2024.

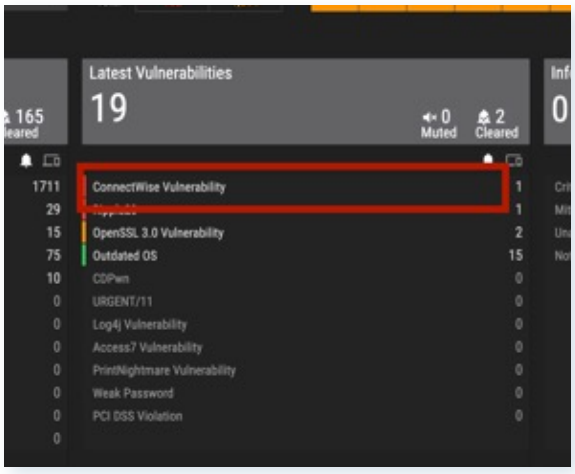
For detailed information and updates on CVE-2024-1709 and CVE-2024-1708, refer to the official CVE database and the advisories provided by ConnectWise and CISA.

How Ordr Is Helping Its Customers To Detect and Respond To This Threat?

1. Updated Ordr Vulnerability database for all customer instances with these latest ConnectWise ScreenConnect CVEs for early identification and patching.



2. Added a new alert type in the “Latest Vulnerabilities” threat card as an easy visual indicator. Ordr analyses the total software installed on all devices and checks for this specific version and matches with this vulnerability after a quick lookup of affected devices.



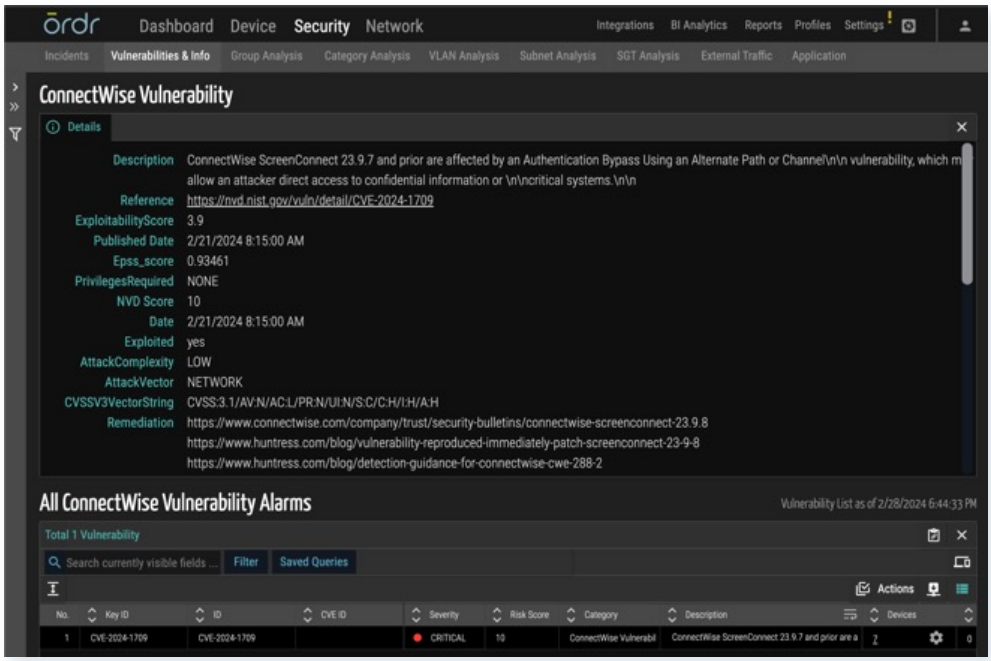
3. Ordr automatically updated the IDS rules corresponding to exploiting these vulnerabilities for real-time detection. After this update, Ordr's IDS engine will start looking for the relevant signatures and automatically add a visual indication in the Ordr security page incident card if there is a match with the signature on the packet stream.

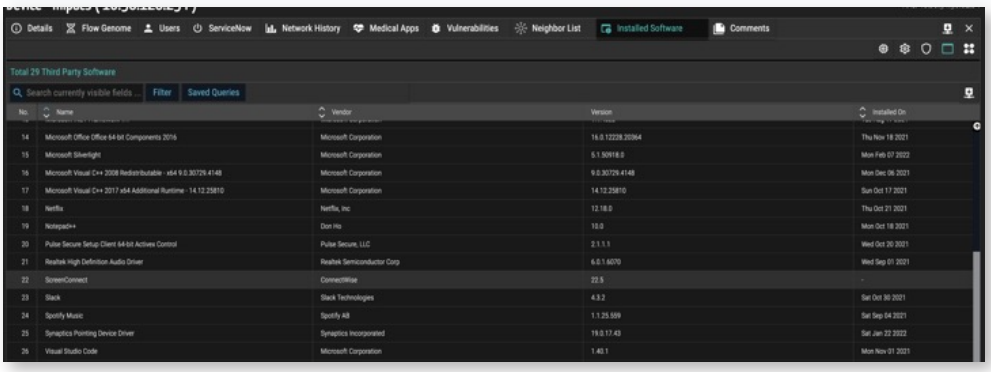
Ordr Detection Details And CVE Lookup

The following are ways to identify if your organization has been exposed to these vulnerabilities and how to mitigate them.

1. **Vulnerability mapping of impacted devices:**

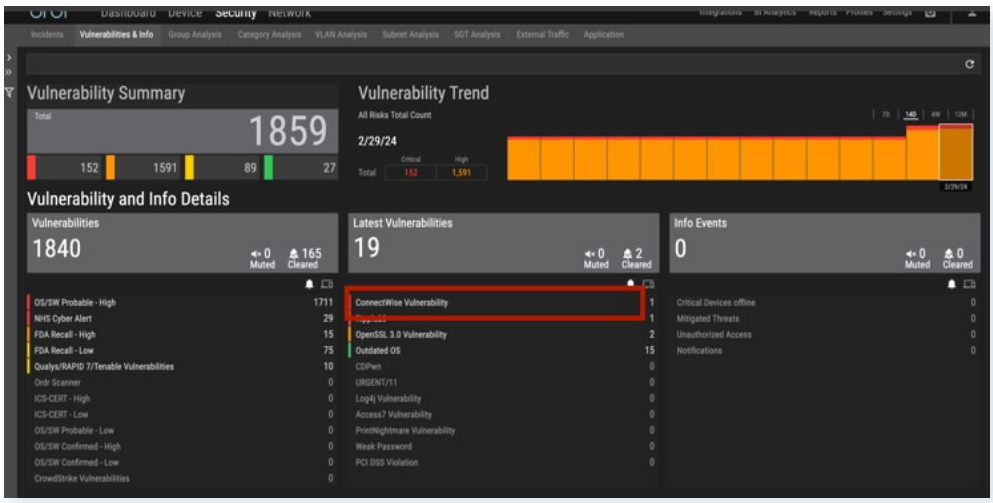
   - Ordr provides visibility into all the devices running ConnectWise applications by mapping applications collected via Ordr Software Inventory Collector or 3rd party integrations like EDR, MDM, MSFT-AD, and others.
   - Ordr also maintains a list of all the software packages installed on the endpoints with exact version numbers and a time stamp on which it was installed and last updated.
   - Ordr matches the software version number against the various Vulnerability Databases to identify vulnerable versions of the ConnectWise ScreenConnect applications.



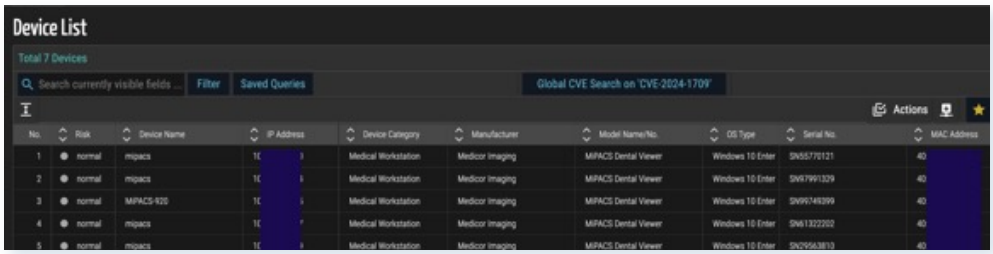


This info can be looked up easily in the following ways:

- Latest Vulnerabilities Card: All devices which run a vulnerable version of the software, are highlighted in the Ordr Vulnerabilities and Info page in the Latest Vulnerabilities card.

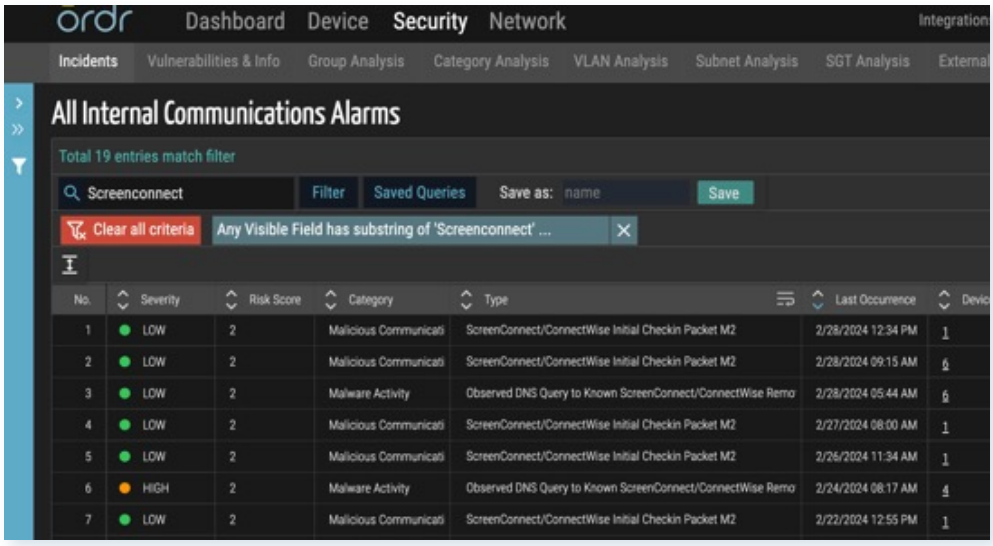


- Global CVE Search: For easy lookup in just a click, customers can search for the CVE ID corresponding to the ScreenConnect vulnerabilities directly from the global CVE search in the Ordr main dashboard page itself.

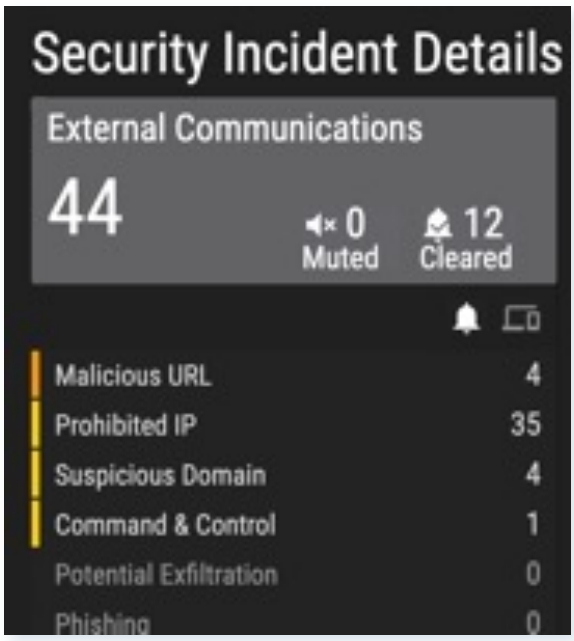


2. **Real-time detection of exploits using IDS, behavioral violation, and threat correlation:**

   Ordr has an IDS engine that can detect this specific vulnerability using analysis of packets transacting over the wire. Ordr IDS signatures have been updated to detect the ConnectWise Screen connect software exploitation.



3. **Generate alerts based on communications to malicious IP/URLs:** In real-time, Ordr's external IP/IOC tracks every communication to prohibited IP/URLs. Ordr uses a cloud-based threat intelligence platform where the list is continuously updated, and all malicious communications alerts are marked accordingly in the Ordr Security Threat Card.

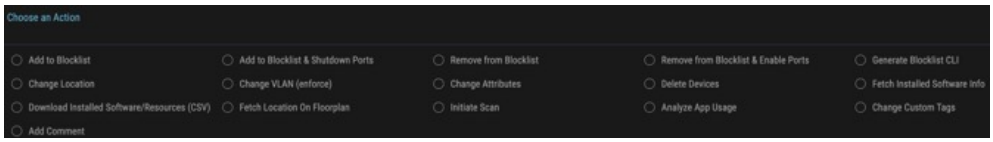


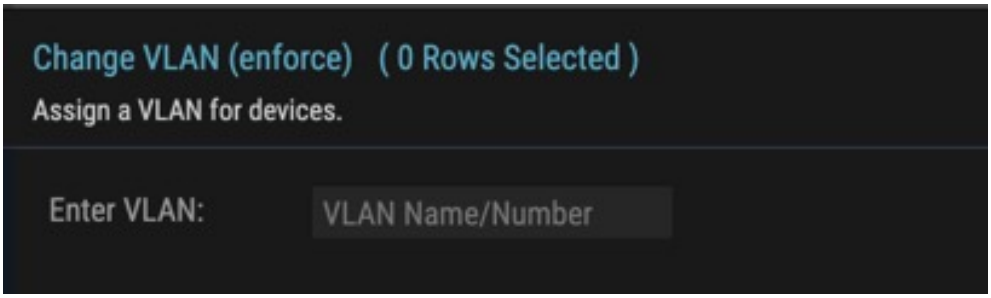
Mitigation Actions to Perform if Detected:

To mitigate the risks associated with CVE-2024-1708 and CVE-2024-1709, several strategies are recommended:

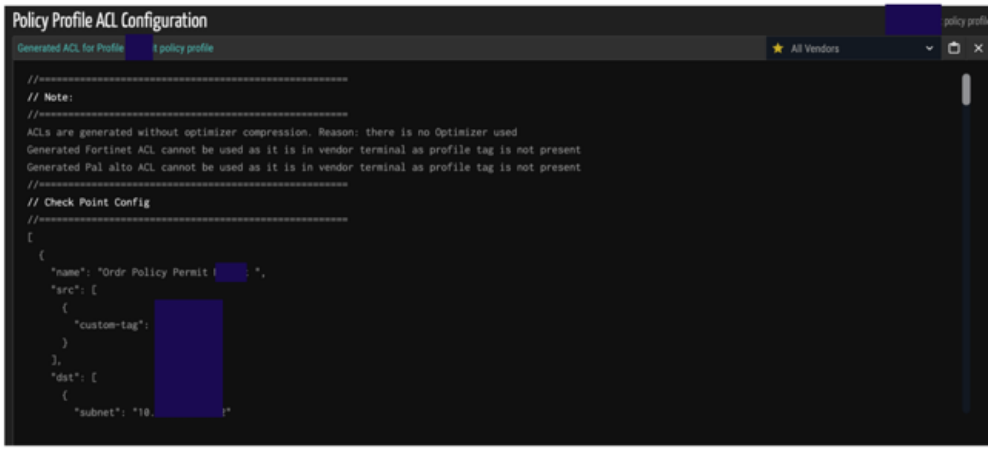
- **Update ConnectWise ScreenConnect software:** Ensure that you are using the latest version of ConnectWise ScreenConnect above version 23.9.8. Updates often include patches for known vulnerabilities, which can prevent exploitation.[1]

- **Reactive rapid threat containment:** Ordr has the capability to rapidly isolate the affected devices if it is deemed to have this vulnerability by putting the device in a quarantine VLAN or denying its connection to the network using automation with a single click. This automation works with almost any flavor of any networking vendors switches or wireless controllers.





- **Pro-active protection:** Ordr's segmentation policies can protect the mission-critical devices. Even if a breach happens, mission-critical devices, for example, medical or devices in ER/OR, can be protected using Ordr policies. Only specific devices over certain protocols can communicate with these mission-critical devices.



Ordr supports integration with multiple industry-leading NAC vendors.

- Stay Informed and Respond Quickly: Regularly check for updates from ConnectWise and security advisories from cybersecurity researchers and organizations like CISA. Responding quickly to vulnerabilities by patching can significantly reduce the risk of exploitation.

Ordr's call to action for customers:

Customers are requested to monitor their environment and quickly identify the presence of Vulnerable devices. Exploitation of the ConnectWise ScreenConnect CVEs mentioned using Ordr's easy lookup methods, then Patch/ Remediate them promptly to safeguard their organization against this rapidly known exploited vulnerability.

Helpful Links:

1. https://ordr.net/
2. https://www.scmagazine.com/news/connectwise-exploit-could-spur-ransomware-free-for-all-expert-warns
3. https://nvd.nist.gov/vuln/detail/CVE-2024-1708
4. https://nvd.nist.gov/vuln/detail/CVE-2024-1709
5. https://www.connectwise.com/company/trust/security-bulletins/connectwise-screenconnect-23.9.8
6. https://www.securityweek.com/black-basta-bl00dy-ransomware-exploiting-recent-screenconnect-flaws/

[1] https://www.huntress.com/blog/a-catastrophe-for-control-understanding-the-screenconnect-authentication-bypass

For assistance with your asset visibility and security needs, visit ordr.net for more information or contact us at info@ordr.net.