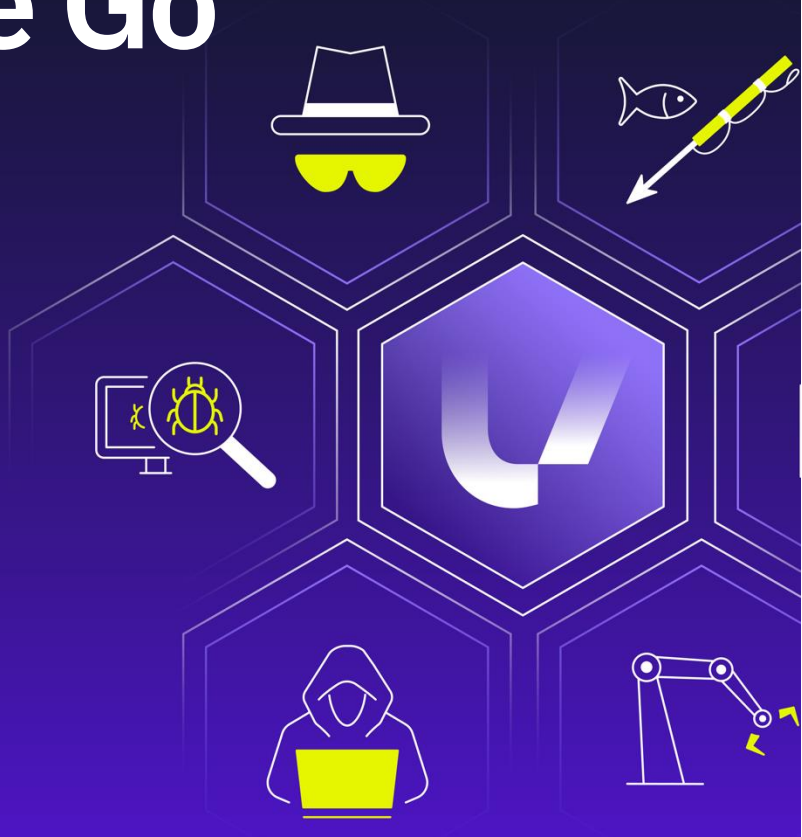
ultraviolet

THREAT REPORT:

ScreenConnect - How We Got Here and Where Do We Go



Services Performed By:
UltraViolet Cyber
Johnathon Moyer
(443) 351-7630
info@uvcyber.com

Published Date:
03/07/2024

Contents

1 Executive Summary

The vulnerabilities related to on-premises versions of ConnectWise's service have been granted a CVSS score of 8.4 and 10, the highest severity available. This is due in no small part to the ease of exploitation and the degree of access it provides threat actors. A simple bit of text at the end of a URL string gets attackers direct admin access to the targeted machine. Updates and hardening techniques have been published, and cloud hosted versions of the ConnectWise service are not vulnerable to this exploit. If you are running ConnectWise on premises and have not updated your instance within the past two weeks, we highly recommend you do so now.

2 Technical Analysis

ScreenConnect is a product used by organizations to allow remote access to hosts within their environment. It is easy to use, requires authentication to access the service and host, and is a popular solution used by many large companies. The related vulnerabilities were documented as CVE-2024-1708: "Improper limitation of a pathname to a restricted directory" and CVE-2024-1709: "Authentication Bypass Using an Alternate Path or Channel". Sophos confirmed LockBit activity related to exploitation of these vulnerabilities on February 22nd, 2024. TrendMicro confirmed similar activity from Black Basta and Bl00dy (formerly LockBit 3.0) ransomware gangs on February 27th, 2024. While law enforcement did initially take down LockBit's servers, the ransomware group was back up and running a week later.

ConnectWise's product introduced both CVE-2024-1708 and CVE-2024-1709 when a pathing issue within their code for 'SetupModule' in the file 'ScreenConnect.Web.dll' contained multiple issues with the .NET framework. For CVE-2024-1708, the 'ScreenConnect.ZipFile.ExtractAllEntries' function did not validate user paths correctly, allowing for a 'ZipSlip' type of attack. This allows a threat actor to upload malicious code to the host via a POST packet. This would be bad enough, but in combination with CVE-2024-1709, the code can run on the host with whatever level of access the threat actor desires.
CVE-2024-1709 works due to an issue with their 'PostMapRequestHandler' function incorrectly handling the 'HttpRequest.Path' property. This allows a GET request to add '/SetupWizard.aspx/' to the header. Affected hosts would then run the setup wizard and allow unauthenticated users to create accounts. Then, the attacker can just log in with those now authorized credentials and use the affected host as a springboard to move laterally within the network, bypassing the DMZ and firewall protections. By combining both vulnerabilities, some groups have already been observed deploying Cobalt Strike beacons, which allow for scanning and exploitation of additional vulnerabilities specific to that host.

3 What UltraViolet Cyber is Doing

- UltraViolet Cyber regularly updates our IOC database to ensure alerting is up to date
- Monitoring commands that are associated with malicious activity from threat actors
- Monitoring network logs for traffic to known malicious sites

4 What Customers Can Do

- If your organization is running a self-hosted version of ConnectWise's v23.9.8 product or earlier, verify that updates related to these vulnerabilities have been applied after appropriate testing
- ConnectWise has removed the license requirement for earlier versions to allow patching of the vulnerabilities

5 References

Black Basta, Bl00dy ransomware gangs join ScreenConnect attacks. Retrieved March 1, 2024, from https://www.bleepingcomputer.com/news/security/black-basta-bl00dy-ransomware-gangs-join-screenconnect-attacks/

CISA Adds One Known Exploited ConnectWise Vulnerability, CVE . Retrieved March 1, 2024, from https://www.cisa.gov/news-events/alerts/2024/02/22/cisa-adds-one-known-exploited-connectwise-vulnerability-cve-2024-1709-catalog

ConnectWise ScreenConnect 23.9.8 security fix. Retrieved March 1, 2024, from https://www.connectwise.com/company/trust/security-bulletins/connectwise-screenconnect-23.9.8

References:

ConnectWise ScreenConnect: Remediation and Hardening Guide. Retrieved March 1, 2024, from https://services.google.com/fh/files/misc/connectwise-screenconnect-remediation-hardening-guide.pdf

Cybercriminal groups actively exploiting . Retrieved March 1, 2024, from https://therecord.media/connectwise-screenconnect-bug-cybercrime-exploitation

Multiple Vulnerabilities in ConnectWise ScreenConnect Could Allow . Retrieved March 1, 2024, from https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-connectwise-screenconnect-could-allow-for-remote-code-execution_2024-023

Shodan Results For ScreenConnect Visible Vulnerable Devices. Retrieved March 1, 2024, from https://www.shodan.io/search?query=%22Server%3A+ScreenConnect%2F23.9.8%22

SOC Landscapes: Insights from SANS. Retrieved March 1, 2024, from https://www.trendmicro.com/en_us/research/24/b/sans-2023-soc-report.html

Sophos X-Ops: "UPDATE: In the last 24 hours, we. Retrieved March 1, 2024, from https://infosec.exchange/@SophosXOps/111975043941611370

Understanding the ConnectWise ScreenConnect CVE-2024-1709 . Retrieved March 1, 2024, from https://www.huntress.com/blog/a-catastrophe-for-control-understanding-the-screenconnect-authentication-bypass