HC3: Sector Alert

February 26, 2024 TLP:CLEAR Report: 202402261300

HPH Entities Urged to Patch High Risk Vulnerabilities from Remote Access Tool

Executive Summary

Following a previous Sector Alert on potential unauthorized access to Healthcare and Public Health (HPH) organizations that use the remote access tool, ScreenConnect, security researchers are now urging organizations to patch high risk vulnerabilities to the software due to an active cyberattack. The impact of the unresolved vulnerabilities has the potential to expand into a mass compromise event for both federal and private industry victims. This Sector Alert provides an update to the exploit, current vulnerabilities, and recommendations for mitigations to detect and protect against future cyberattacks.

Report

The victim software organization was made aware of the vulnerabilities on February 13, but publicly disclosed details of them in an advisory on February 19. While it initially stated that there was no evidence of exploitation in the wild at the time, it did confirm later that it had received updates of compromised accounts. The flaw is described as an authentication bypass vulnerability that could allow an attacker to remotely steal confidential data from vulnerable servers or deploy malicious code, such as malware.

The two vulnerabilities affect the ScreenConnect remote desktop access product. The more serious flaw, CVE-2024-1709, is rated a peak CVSS security score of 10 and stems from an authentication bypass weakness. The second flaw, CVE-2024-1708, is a high-severity path traversal vulnerability that is susceptible only to attackers with high privileges.

While the victim organization declined to say how many customers are currently affected, they did add that 80% of customer environments are cloud-based, and that they were patched automatically within 48 hours. Several private cybersecurity organizations also conducted their own analysis of the impact of the vulnerabilities. At the time, Shodan.io, the internet of things search engine, indicated that more than 8,000 ScreenConnect servers are exposed to the internet, and only 5% of them (approximately 430 servers) were running the patched version 23.9.8. Palo Alto Networks' Unit42 also observed that more than 16,000 distinct IPs are likely vulnerable and urged organizations to urgently patch them. Huntress stated that upwards of 8,800 servers of the victim organization remain vulnerable to exploitation.

Earlier this year, U.S. government agencies CISA and the National Security Agency (NSA) warned in a joint advisory that they had observed a "widespread cyber campaign involving the malicious use of legitimate remote monitoring and management (RMM) software" – including ScreenConnect – to target multiple Federal civilian executive branch agencies. This follows a previous campaign from October to November 2023, in which threat actors abused ScreenConnect for initial access to victim organizations. In that campaign, threat actors proceeded to take several steps, including installing additional remote access tools such as ScreenConnect or AnyDesk instances, to ensure persistent access to the environment. While the threat actor(s) leveraged local ScreenConnect instances used by a pharmacy supply chain and management systems solution provider that is present in all 50 states, the impact of that campaign is still unknown.

HC3: Sector Alert

February 26, 2024 TLP:CLEAR Report: 202402261300

Vulnerabilities

CVE-2024-1709 (Last Modified February 22, 2024)		
Description	Vulnerability	ConnectWise ScreenConnect 23.9.7 and prior are affected by an Authentication Bypass Using an Alternate Path or Channel vulnerability, which may allow an attacker direct access to confidential information or critical systems.
	CVSS Score	10.0 CRITICAL
	Required Action	Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.
Weakness Enumeration	CWE-ID	NVD-CWE-Other
	CWE Name	Other
	Source	NIST
Weakness Enumeration	CWE-ID	CWE-288
	CWE Name	Authentication Bypass Using an Alternate Path of Channel
	Source	CISA

CVE-2024-1708 (Last Modified February 22, 2024)		
Description	Vulnerability	ConnectWise ScreenConnect 23.9.7 and prior are affected by a path-traversal vulnerability, which may allow an attacker the ability to execute remote code or directly impact confidential data or critical systems.
	CVSS Score	8.4 HIGH
Weakness Enumeration	CWE-ID	CWE-22
	CWE Name	Improper Limitation of a Pathname to a Restricted Directory (‘Path Traversal’)
	Source	NIST and CISA

Defense and Mitigations

The issues impact ScreenConnect version 23.9.7 and prior. To protect themselves, organizations that currently utilize ScreenConnect should upgrade to version 23.9.8 immediately to patch their systems, then hunt for signs of exploitation. Recommendations from the previous CISA and NSA advisory include organizations taking concerted steps to safeguard their infrastructure. At a minimum, cybersecurity researchers were encouraged to enhance endpoint monitoring, ensure robust cybersecurity frameworks, and initiate proactive threat hunting to mitigate potential threat actor intrusions.

The Way Forward

The full impact of this cyberattack is currently unknown. However, as stated on the victim organization’s own website, remote access technology is offered to more than a million small to medium-sized businesses, indicating that the potential for adverse effects could be likely to current users. Any discovery of active exploitation should be taken seriously and investigated promptly. Given the potential implications of such an attack in the HPH sector, particularly regarding patient data, privacy, and availability of critical services, a comprehensive response is essential.

In addition to a HC3 Analyst Note on Healthcare Sector DDoS Guide on how to safeguard against ransomware/extortion attacks, some cyber security professionals advise that the healthcare industry acknowledge the ubiquitous threat of cyberwar against them and recommend that their cybersecurity teams implement the following steps:

- Educate and train staff to reduce the risk of social engineering attacks via email and network access.
- Assess enterprise risk against all potential vulnerabilities and prioritize implementing the security plan with the necessary budget, staff, and tools.
- Develop a cybersecurity roadmap that everyone in the healthcare organization understands.

At no cost, the Cybersecurity & Infrastructure Security Agency (CISA) also offers Cyber Hygiene Vulnerability Scanning services to federal, state, local, tribal and territorial governments, as well as public and private sector critical infrastructure organizations. This service helps organizations monitor and evaluate their external network posture.

The probability of cyber threat actors targeting the healthcare industry remains high. Prioritizing security by maintaining awareness of the threat landscape, assessing their situation, and providing staff with tools and resources necessary to prevent a cyberattack remains the best way forward for healthcare organizations.

Relevant HHS Reports

HC3: Analyst Note – Healthcare Sector DDoS Guide (February 13, 2023)

HC3: Sector Alert – Possible Threat of Unauthorized Access to HPH Organizations from Remote Access Tool (January 22, 2024)

References

"A Catastrophe For Control: Understanding the ScreenConnect Authentication Bypass (CVE-2024-1709 & CVE-2024-1708)." Huntress. February 21, 2024. https://www.huntress.com/blog/a-catastrophe-for-control-understanding-the-screenconnect-authentication-bypass

Bagwe, Mihir. "ScreenConnect Servers at High Risk as POC Becomes Public." Bank Info Security. February 21, 2024. https://www.bankinfosecurity.com/screenconnect-servers-at-high-risk-as-poc-becomes-public-a-24413

Chirgwin, Richard. "ConnectWise patches critical ScreenConnect vulnerability." ITnews. February 22, 2024. https://www.itnews.com.au/news/connectwise-patches-critical-screenconnect-vulnerability-605354

"CVE-2024-1708 Detail." National Institute of Standards and Technology - National Vulnerability Database. February 22, 2024. https://nvd.nist.gov/vuln/detail/CVE-2024-1708

"CVE-2024-1709 Detail." National Institute of Standards and Technology - National Vulnerability Database. February 22, 2024. https://nvd.nist.gov/vuln/detail/CVE-2024-1709

Muncaster, Phil. "Ransomware Warning as CVSS 10.0 ScreenConnect Bug is Exploited." Infosecurity Magazine. February 22, 2024. https://www.infosecurity-magazine.com/news/ransomware-cvss-100-screenconnect/

Paganini, Pierluigi. “ConnectWise Fixed Critical Flaws in ScreenConnect Remote Access Tool.” Security Affairs. February 20, 2024. https://securityaffairs.com/159416/security/connectwise-fixed-critical-bugs.html

Page, Carly. “Researchers warn high-risk ConnectWise flaw under attack is ‘embarrassingly easy’ to exploit.” TechCrunch. February 21, 2024. https://techcrunch.com/2024/02/21/researchers-warn-high-risk-connectwise-flaw-under-attack-is-embarrassingly-easy-to-exploit/

Page, Carly. “US federal agencies hacked using legitimate remote desktop tools.” TechCrunch. January 26, 2023. https://techcrunch.com/2023/01/26/us-federal-agencies-hacked-remote-access-tools/

“Protecting Against Malicious Use of Remote Monitoring and Management Software.” Cybersecurity & Infrastructure Security Agency. January 26, 2023. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-025a

Seals, Tara. “Critical ConnectWise RMM Bug Poised for Exploitation Avalanche.” DarkReading. February 21, 2024. https://www.darkreading.com/remote-workforce/critical-connectwise-rmm-bug-poised-exploitation-avalanche

Contact Information

If you have any additional questions, we encourage you to contact us at HC3@hhs.gov.