Office of
Information Security
Securing One HHS

Health Sector Cybersecurity Coordination Center

HC3: Sector Alert

January 22, 2024 TLP:CLEAR Report: 202401221700

Possible Threat of Unauthorized Access to HPH Organizations from Remote Access Tool

Executive Summary

Security researchers are warning that Healthcare and Public Health (HPH) organizations that use the remote access tool ScreenConnect could be adversely affected or targeted by threat actors. The impact of potential unauthorized access on both federal and private industry victims, many of which rely on this tool, would be a concerning development for the healthcare sector. This Sector Alert provides a technical overview of issues concerning the remote access tool, IOCs, and recommendations for mitigations to detect and protect against future cyberattacks.

Report

Between October 28 and November 8, 2023, an unknown threat actor abused a locally hosted instance of a widely-used remote access tool, ScreenConnect, for initial access to victim organizations. After initial access, the attacker proceeded to take several steps, including installing additional remote access tools such as ScreenConnect or AnyDesk instances, to ensure persistent access to the environment. A cybersecurity firm identified the attacks on endpoints from two distinct healthcare organizations and activity indicating network reconnaissance in preparation of attack escalation. On November 14, the vendor of ScreenConnect confirmed that the threat actor gained access via an unmanaged on-prem instance that had not been updated since 2019, going against recommended best practices. The impact, while still unknown, could be substantial, as the threat actor leveraged local ScreenConnect instances used by a pharmacy supply chain and mangement systems solution provider that is present in all 50 states.

The attacks featured similar tactics, techniques, and procedures (TTPs), including the downloading of a payload named *test.xml*, indicating that the same actor was behind all observed incidents. The compromised endpoints operated on a Windows Server 2019 system, belonging to two distinct organizations, a pharmaceutical firm and a healthcare provider, the common link between them being a ScreenConnect instance. The remote access tool was then used to install additional payloads, to execute commands, to transfer files, and to install AnyDesk. The hackers also tried to create a new user account for persistent access. It is still unclear if the pharmacy supply chain and mangement systems solution provider suffered a breach, if the credentials to one of their accounts were compromised, or if the attackers exploited a different mechanism.

Indicators of Compromise

IP Address	Hosting Provider	Hosting Location	Function
119.91.138[.]133	Tencent Computer Systems	CN	Primary infrastructure for storing and retrieving post-access payloads
185.12.45[.]98	Private Layer Inc	PA	Connecting server associated with malicious ScreenConnect instance D
45.66.230[.]146	Delis LLC	NL	Connecting server associated with malicious ScreenConnect instance C
2.57.149[.]103	Red Byte LLC	PL	Hosting server for AnyDesk MSI installation

Additional Files & Payloads

Name	Function
SHA256	test.xml 9f42bf3a61faaab8f86abb3c7f9db417bffb3474a55169a4efb1d2386545e4e8
C# payload designed to load Meterpreter into victim memory	
a.msi 70f865a7f8a01356685b17abdf6ac738e9a9098f1ae2d5a34cfa3610cb28fc56	
AnyDesk MSI installer	
s.msi 8c3b4febe58df0a01126d78109f52035d34a4e03f02b5d4fca3e4d94f3f657b3	
ScreenConnect MSI installer	

File Paths and Names

C:\programdata\a.msi
C:\programdata\test.xml
C:\Users\Administrator\Documents\a.msi
S.msi
C:\Users\manager\Documents\ConnectWiseControl\Files\Advanced_IP_Scanner_2.5.4594.1.exe
C:\Program Files (x86)\ScreenConnect Client (<unique identifier>)\ScreenConnect.ClientService.exe

Defense and Mitigations

As the compromised endpoints operated on an unmanaged instance of a Windows Server 2019 system, it is recommended that organizations take concerted steps to safeguard their infrastructure. At a minimum, cybersecurity researchers encourage enhanced endpoint monitoring, robust cybersecurity frameworks, and proactive threat hunting to mitigate potential threat actor intrusions.

The Way Forward

Pharmacies and other healthcare organizations that may be clients of the pharmacy supply chain and mangement systems solution provider should immediately examine their systems and networks for the above IOCs. Any discovery of these should be taken seriously and investigated promptly. Given the potential implications of such a breach in the HPH sector, particularly regarding patient data, privacy, and availability of critical services, a comprehensive response is essential.

The full extent of this incident is still unknown and being investigated to determine its potential wider impact. While no attribution is presently known, organizations can still take proactive steps to protect themselves and mitigate against potential future incidents.

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 your situation, and providing staff with tools and resources necessary to prevent a cyberattack remain the best ways forward for healthcare organizations.

Relevant HHS Reports

HC3: Alert – 2021 Trends Show Increased Globalized Threat of Ransomware (February 9, 2022)

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

HC3: Analyst Note – Health Sector Ransomware Trends for Third Quarter 2021 (October 13, 2021)

HC3: Threat Brief – Ransomware Trends in Q1 2022 (May 5, 2022)

HC3: Threat Brief – Ransomware Trends 2021 (June 3, 2021)

References

"Bitter Pill: Third-Party Pharmaceutical Vendor Linked to Pharmacy and Health Clinic Cyberattack." Huntress. November 9, 2023. https://www.huntress.com/blog/third-party-pharmaceutical-vendor-linked-to-pharmacy-and-health-clinic-cyberattack

"Remote access tool leveraged to compromise US healthcare organizations." SC Media. November 13, 2023. https://www.scmagazine.com/brief/remote-access-tool-leveraged-to-compromise-us-healthcare-organizations

Toulas, Bill. "Hackers breach healthcare orgs via ScreenConnect remote access." BleepingComputer. November 10, 2023. https://www.bleepingcomputer.com/news/security/hackers-breach-healthcare-orgs-via-screenconnect-remote-access/

Contact Information

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

We want to know how satisfied you are with the resources HC3 provides. Your answers will be anonymous, and we will use the responses to improve all future updates, features, and distributions. Share Your Feedback