American Hospital Association™
Advancing Health in America

Cybersecurity Advisory

February 26, 2024

UPDATE: New Bulletin on Change Healthcare Cyberattack Highlights Network Connectivity Issues and Indicators of Compromise

TLP:WHITE [i]

Change Healthcare, a health care technology company that is part of Optum and owned by UnitedHealth Group, continues to experience a cyberattack that is having effects on the entire health care system. Since the cyberattack began Feb. 21, the AHA has been sharing information with members to help them navigate this evolving incident.

As part of those efforts, Health-ISAC, which AHA partners with closely, today issued a bulletin to provide additional information regarding maintaining network connectivity with UnitedHealth Group, Optum and UnitedHealthcare, and indicators of compromise. The following issues and recommendations are outlined in the Health-ISAC bulletin and consistent with guidance that AHA has issued about this incident.

Please share this advisory with your organization's information technology and/or cybersecurity teams.

NETWORK CONSIDERATIONS

Change Healthcare has indicated it has taken appropriate action to contain the incident so that customers and partners do not need to sever network connections to available vital services.

Change Healthcare continues to say on its webpage "that we have a high-level of confidence that Optum, UnitedHealthcare and UnitedHealth Group systems have not been affected by this Issue." The AHA continues to be encouraged by this public statement, and health care organizations should give this statement strong consideration.

Accordingly, the AHA and Health-ISAC continue to recommend that organizations immediately reevaluate their risk of keeping any network services shut down to Optum, Change Healthcare, UnitedHealthcare and/or UnitedHealth Group which has been deemed safe by them. Each health care organization should continue to monitor and independently evaluate information provided by Change Healthcare to inform its own risk-based decisions regarding nonimpacted systems.

When considering connectivity to nonimpacted Change Healthcare systems, each health care organization should weigh possible clinical disruptions and business

impacts caused by severing the connection to nonimpacted Optum, Change Healthcare, UnitedHealthcare and/or United Health Group systems.

The AHA and Health-ISAC continue to recommend that all health care organizations maintain disconnection from applications specified by Change Healthcare that remain unavailable due to this cyberattack, as identified on the Change Healthcare application status page.

The AHA independently provided the above connectivity guidance on Feb. 23 during a national call with the field and again in a Feb. 24 Cybersecurity Advisory.

INDICATORS OF COMPROMISE

Today's Health-ISAC bulletin cites information published by cyber intelligence firm RedSense, saying that Change Healthcare, along with other organizations, fell victim to exploitation of the recently announced ConnectWise ScreenConnect vulnerabilities (CVE-2024-1708 and CVE-2024-1709). As the incident is still under investigation, it is not possible to confirm the attack details.

Regardless of what happened at Change Healthcare, RedSense anticipates more organizations will be compromised as the ScreenConnect exploit is apparently fairly trivial to execute. **If your organization has ConnectWise ScreenConnect in your environment, please review the following indicators and recommendations contained below in red from the Health-ISAC bulletin:**

Atomic IOCs, traffic to/from these could indicate compromise-

- 155.133.5[.]15
- 155.133.5[.]14
- 118.69.65[.]60
- 118.69.65[.]61
- 207.148.120[.]105
- 192.210.232[.]93
- 159.203.191[].1

Additional IOCs, these could indicate compromise as well

- presence of User.xml in the Windows ScreenConnect path (this file generally equates to an owned server, recommend to isolate endpoint, inspect this file and look for RCE)
- Examine this file on the server hosting connectwise/screen connect: C:\Program Files (x86)\ScreenConnect\App_Data\User.xml

Evaluate the "<name>" field along with the "<CreationDate>" field. If a user was recently created, review their <roles> field. If the role is 'admin' related, you probably have been compromised.

- The attack chain bypasses 2-factor authentication via brute force before executing local commands. The threat actors initially create an account called ‘cloudadmin’. The ‘cloudadmin’ account then creates a ‘test@2021’ user. The ‘test@2021’ user pings google.com. Next, the threat actors attempt to establish a connection over HTTPS to transfer[.]sh, a web-based file-sharing service, most likely using the command line.

Additional Background
On February 19, 2024, ConnectWise alerted users of a remote code execution (RCE) flaw that can be leveraged to bypass authentication in ScreenConnect servers. The CVEs associated with these actively exploited vulnerabilities are CVE-2024-1708 (CVSS 8.4) and CVE-2024-1709 (CVSS 10.0). Still, ConnectWise has advised its customers to patch their ScreenConnect servers immediately against the critical vulnerability to prevent RCE attacks.

The critical vulnerability patched in the ConnectWise ScreenConnect remote desktop software has been observed being exploited in the wild. ScreenConnect is a popular remote desktop software with both on-premise and in-cloud deployments. The exploited flaw allows attackers to bypass authentication and gain remote code execution on systems.

These Indicators of Compromise (IOCs) and Tactics, Techniques, and Procedures (TTPs) have been pushed into the H-ISAC AMBER MEMBERS collection on the Health-ISAC Indicator Threat Sharing (HITS) automated systems for STIX and TAXII subscribers.

Mitigation Practices:
Security researchers recommend that all organizations running any affected version immediately update the software. According to ConnectWise, due to the likelihood of these devices being exploited in attacks, it is strongly advised that you update your devices as soon as possible.

PAST AHA ADVISORIES AND ACTIONS TO KEEP MEMBERS INFORMED

The AHA has kept members informed throughout this incident.

- On Feb. 22, we issued an initial Cybersecurity Advisory to alert hospitals and health systems to the attack and recommended steps hospitals and health systems could take.
- On Feb. 23, we hosted a call with leaders from the Department of Health and Human Services, Cybersecurity and Infrastructure Security Agency, and Federal Bureau of Investigation to provide the latest information on the incident and answer questions.

- On Feb. 24, we issued an updated Cybersecurity Advisory with additional details about the incident, recommendations for hospitals to consider, and actions the AHA is undertaking.
- On Feb. 25, we issued a new Cybersecurity Advisory with additional information about the indicators of compromise to assist network defenders with conducting an indicator sweep within their environment to determine whether their network has been compromised.

NEXT STEPS

The AHA will continue to keep you updated on this situation. Please send any technical, financial and/or clinical impact or related technical threat intelligence on a confidential basis to John Riggi, AHA's national advisor for cybersecurity and risk, at jriggi@aha.org. The AHA maintains close contact with the FBI, HHS and CISA and will share cyber threat intelligence with them without attribution to your organization, unless you specify permission to be identified. **If you have identified any of these indicators of compromise on your network, or are experiencing a ransomware attack, contact your local FBI field office or FBI 24/7 Cyber Watch at 855-292-3937 and describe any delay or disruption to care delivery.**

FURTHER QUESTIONS

If you have further questions, please contact Riggi at jriggi@aha.org. For the latest cyber threat intelligence and resources, visit www.aha.org/cybersecurity.

---

[i] **TLP:WHITE** Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.