Change Healthcare / Optum Network Connectivity and Additional Recommendations

TLP: WHITE This report may be shared without restriction. For Health-ISAC Members be sure to download the full version of the report from the Health-ISAC Threat Intelligence Portal (HTIP). Contact Membership Services for assistance.

Threat Bulletins **TLP:WHITE** **Alert Id: c8449b97** **2024-02-26 11:32:59**

Health-ISAC is sharing this Threat Bulletin to provide additional information regarding the following:
1. Maintaining network connectivity with UnitedHealth Group, Optum, and UnitedHealthcare.
2. Indicators of Compromise (IOCs)

Update June 10, 2024
As Health-ISAC learned in this BleepingComputer article dated February 28, 2024, the BlackCat/ALPHV ransomware gang officially claimed responsibility for the cyberattack on Change Healthcare. BlackCat also denied using a critical ScreenConnect auth bypass flaw for initial access.

Original Bulletin:

1) Network Connectivity

On Wednesday, February 21, Change Healthcare began experiencing a cyber security issue and isolated its systems to prevent further impact. Optum, UnitedHealthcare, and UnitedHealth Group (UHG) systems were not affected by the issue, according to information provided by UHG. UHG has indicated they have taken appropriate action to contain the incident so that customers and partners do not need to sever network connections and disrupt vital services. Health-ISAC recommends the following:

•Change Healthcare continues to say on its webpage that they "... have a high-level of confidence that Optum, UnitedHealthcare and UnitedHealth Group systems have not been affected by this Issue." Organizations should 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.
•Continue to keep connections severed with Change Healthcare given that as of February 25, 2024, that environment has not been deemed safe by UHG/Optum

As part of the risk evaluation, healthcare organizations should consider the impacts of severing connectivity to Optum, which includes but is not limited to loss of prior procedure authorizations, electronic prescribing, and other patient care functions. Ultimately, your organization should make its own determination on whether or not to block Optum specifically while considering all the risks and consequences of doing so.

2) Indicators of Compromise (IOCs)

According to information published by cyber intelligence firm RedSense, 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. We would expect to see additional victims in the coming days. If your organization has ConnectWise ScreenConnect in your environment, please review the indicators and recommendations below.

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.

Reference(s): RedSense, Connectwise, Health-ISAC , CSO Online

Report Source(s): Health-ISAC

Incident Date: Feb 21, 2024 (UTC)

Tags: UHG, ChangeHealthcare, Optum, RedSense, ConnectWise

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

F**or Questions and/or Comments:**

Please email us at contact@h-isac.org

Conferences, Webinars, and Summits:

https://h-isac.org/events/

Share Threat Intel:

For guidance on sharing indicators with Health-ISAC via CSAP, please visit the Knowledge Base article CSAP Share Threat Intel Documentation at the link address provided here: https://health-isac.cyware.com/webapp/user/knowledge-base. Additionally, this collaborative medium provides opportunities for attributed or anonymous sharing across ISACs and other cybersecurity-related entities.

Access the Health-ISAC Intelligence Portal:

Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Cyware.