CYBERSECURITY ADVISORY

Co-Authored by:

Product ID: AA25-163A

June 12, 2025

Ransomware Actors Exploit Unpatched SimpleHelp Remote Monitoring and Management to Compromise Utility Billing Software Provider

Summary

The Cybersecurity and Infrastructure Security Agency (CISA) is releasing this advisory in response to ransomware actors leveraging unpatched instances of a vulnerability in SimpleHelp Remote Monitoring and Management (RMM) to compromise customers of a utility billing software provider. This incident reflects a broader pattern of ransomware actors targeting organizations through unpatched versions of SimpleHelp RMM since January 2025.

SimpleHelp versions 5.5.7 and earlier contain several vulnerabilities, including CVE-2024-57727—a path traversal vulnerability.[1] Ransomware actors likely leveraged CVE-2024-57727 to access downstream customers' unpatched SimpleHelp RMM for disruption of services in double extortion compromises.[1]

CISA added CVE-2024-57727 to its Known Exploited Vulnerabilities (KEV) Catalog on Feb. 13, 2025.

CISA urges software vendors, downstream customers, and end users to immediately implement the **Mitigations** listed in this advisory based on confirmed compromise or risk of compromise.

To report suspicious or criminal activity related to information found in this Cybersecurity Advisory, 24/7 Operations Center at Report@cisa.gov or (888) 282-0870. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact.

This document is marked TLP:CLEAR. Disclosure is not limited. Sources may use TLP:CLEAR when information carries minimal or no forseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be distributed without restriction. For more information on the Traffic Light Protocol, see Traffic Light Protocol (TLP) Definitions and Usage.

Mitigations

CISA recommends organizations implement the mitigations below to respond to emerging ransomware activity exploiting SimpleHelp software. These mitigations align with the Cross-Sector Cybersecurity Performance Goals (CPGs) developed by CISA and the National Institute of Standards and Technology (NIST). The CPGs provide a minimum set of practices and protections that CISA and NIST recommend all organizations implement. CISA and NIST based the CPGs on existing cybersecurity frameworks and guidance to protect against the most common and impactful threats, tactics, techniques, and procedures. Visit CISA's CPGs webpage for more information on the CPGs, including additional recommended baseline protections. These mitigations apply to all critical infrastructure organizations.

Vulnerable Third-Party Vendors

If SimpleHelp is embedded or bundled in vendor-owned software or if a third-party service provider leverages SimpleHelp on a downstream customer's network, then identify the SimpleHelp server version at the top of the file `<file_path>/SimpleHelp/configuration/serverconfig.xml`. If version 5.5.7 or prior is found or has been used since January 2025, third-party vendors should:

1. Isolate the SimpleHelp server instance from the internet or stop the server process.
2. Upgrade immediately to the latest SimpleHelp version in accordance with SimpleHelp's security vulnerability advisory.[2]
3. Contact your downstream customers to direct them to take actions to secure their endpoints and undertake threat hunting actions on their network.

Vulnerable Downstream Customers and End Users

Determine if the system is running an unpatched version of SimpleHelp RMM either directly or embedded in third-party software.

SimpleHelp Endpoints

Determine if an endpoint is running the remote access (RAS) service by checking the following paths depending on the specific environment:

- Windows: `%APPDATA%\JWrapper-Remote Access`
- Linux: `/opt/JWrapper-Remote Access`
- MacOs: `/Library/Application Support/JWrapper-Remote Access`

If RAS installation is present and running, open the `serviceconfig.xml` file in `<file_path>/JWrapper-Remote Access/JWAppsSharedConfig/` to determine if the registered service is vulnerable. The lines starting with `<ConnectTo` indicate the server addresses where the service is registered.

SimpleHelp Server

Determine the version of any SimpleHelp server by performing an HTTP query against it. Add `/allversions` (e.g., `https://simple-help.com/allversions`) to query the URL for the version page. This page will list the running version.

If an unpatched SimpleHelp version 5.5.7 or earlier is confirmed on a system, organizations should conduct threat hunting actions for evidence of compromise and continuously monitor for unusual inbound and outbound traffic from the SimpleHelp server. **Note:** This is not an exhaustive list of indicators of compromise.

1. Refer to SimpleHelp's guidance to determine compromise and next steps.[3]
2. Isolate the SimpleHelp server instance from the internet or stop the server process.
3. Search for any suspicious or anomalous executables with three alphabetic letter filenames (e.g., `aaa.exe`, `bbb.exe`, etc.) with a creation time after January 2025. Additionally, perform host and network vulnerability security scans via reputable scanning services to verify malware is not on the system.
4. Even if there is no evidence of compromise, users should immediately upgrade to the latest SimpleHelp version in accordance with SimpleHelp's security vulnerabilities advisory.[4]

If your organization is unable to immediately identify and patch vulnerable versions of SimpleHelp, apply appropriate workarounds. In this circumstance, CISA recommends using other vendor-provided mitigations when available. These non-patching workarounds should not be considered permanent fixes and organizations should apply the appropriate patch as soon as it is made available.

Encrypted Downstream Customers and End Users

If a system has been encrypted by ransomware:

1. Disconnect the affected system from the internet.
2. Use clean installation media (e.g., a bootable USD drive or DVD) to reinstall the operating system. Ensure the installation media is free from malware.
3. Wipe the system and only restore data from a clean backup. Ensure data files are obtained from a protected environment to avoid reintroducing ransomware to the system.

CISA urges you to promptly report ransomware incidents to a local FBI Field Office, FBI's Internet Crime Compliant Center (IC3), and CISA via CISA's 24/7 Operations Center (report@cisa.gov or 888-282-0870).

Proactive Mitigations to Reduce Risk

To reduce opportunities for intrusion and to strengthen response to ransomware activity, CISA recommends customers of vendors and managed service providers (MSPs) implement the following best practices:

- Maintain a robust asset inventory and hardware list [CPG 1.A].

- Maintain a clean, offline backup of the system to ensure encryption will not occur once reverted. Conduct a daily system backup on a separate, offline device, such as a flash drive or external hard drive. Remove the device from the computer after backup is complete [CPG 2.R].
- Do not expose remote services such as Remote Desktop Protocol (RDP) on the web. If these services must be exposed, apply appropriate compensating controls to prevent common forms of abuse and exploitation. Disable unnecessary OS applications and network protocols on internet-facing assets [CPG 2.W].
- Conduct a risk analysis for RMM software on the network. If RMM is required, ask third-party vendors what security controls are in place.
- Establish and maintain open communication channels with third-party vendors to stay informed about their patch management process.
- For software vendors, consider integrating a Software Bill of Materials (SBOM) into products to reduce the amount of time for vulnerability remediation.
    - An SBOM is a formal record of components used to build software. SBOMs enhance supply chain risk management by quickly identifying and avoiding known vulnerabilities, identifying security requirements, and managing mitigations for vulnerabilities. For more information, see CISA's SBOM page.

Resources

- **Health-ISAC:** Threat Bulletin: SimpleHelp RMM Software Leveraged in Exploitation Attempt to Breach Networks
- **Arctic Wolf:** Arctic Wolf Observes Campaign Exploiting SimpleHelp RMM Software for Initial Access
- **CISA:** #StopRansomware Guide

Reporting

Your organization has no obligation to respond or provide information back to FBI in response to this advisory. If, after reviewing the information provided, your organization decides to provide information to FBI, reporting must be consistent with applicable state and federal laws.

FBI is interested in any information that can be shared, to include boundary logs showing communication to and from foreign IP addresses, a sample ransom note, communications with threat actors, Bitcoin wallet information, decryptor files, and/or a benign sample of an encrypted file.

Additional details of interest include a targeted company point of contact, status and scope of infection, estimated loss, operational impact, transaction IDs, date of infection, date detected, initial attack vector, and host- and network-based indicators.

CISA and FBI do not encourage paying ransom as payment does not guarantee victim files will be recovered. Furthermore, payment may also embolden adversaries to target additional organizations, encourage other criminal actors to engage in the distribution of ransomware, and/or fund illicit activities. Regardless of whether you or your organization have decided to pay the ransom, FBI and CISA urge you to promptly report ransomware incidents to FBI's Internet Crime Complain Center (IC3), a local FBI Field

Office, or CISA via the agency's Incident Reporting System or its 24/7 Operations Center (report@cisa.gov) or by calling 1-844-Say-CISA (1-844-729-2472).

SimpleHelp users or vendors can contact support@simple-help.com for assistance with queries or concerns.

Disclaimer

The information in this report is being provided "as is" for informational purposes only. CISA does not endorse any commercial entity, product, company, or service, including any entities, products, or services linked within this document. Any reference to specific commercial entities, products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favor by CISA.

Version History

June 12, 2025: Initial version.

Notes

[1] Anthony Bradshaw, et. al., "DragonForce Actors Target SimpleHelp Vulnerabilities to Attack MSP, Customers," *Sophos News*, May 27, 2025, https://news.sophos.com/en-us/2025/05/27/dragonforce-actors-target-simplehelp-vulnerabilities-to-attack-msp-customers/.

[2] For instructions for upgrading to the latest version of SimpleHelp, see SimpleHelp's security vulnerability advisory.

[3] To determine possibility of compromise and next steps, see SimpleHelp's guidance.

[4] For instructions for upgrading to the latest version of SimpleHelp, see SimpleHelp's security vulnerability advisory.