American Hospital Association™
Advancing Health in America

# Cybersecurity Advisory

TLP:CLEAR*

January 29, 2025

# SimpleHelp Remote Access Software Vulnerable to Ransomware Attacks

The AHA in collaboration with Health-ISAC and the field identified attempted and ongoing ransomware attacks potentially due to SimpleHelp remote monitoring and management (RMM) software vulnerabilities.

Based on the potential threat and impact on patient care, the AHA requested and is distributing the threat intelligence from Health-ISAC detailed below.

It is strongly recommended that all instances of the SimpleHelp application within health care organizations be identified and appropriate patches be applied per the bulletin guidance. It is also strongly recommended that health care organizations ensure that all third-party and business associates using SimpleHelp, such as remote radiology service providers, also apply appropriate patches.

**Please share this information with your IT and cyber infrastructure teams.**

## RECOMMENDATIONS

- **Immediate software update.** Users of SimpleHelp RMM software should upgrade to the latest versions to address identified vulnerabilities.
- **Share the Health-ISAC recommendations** with your IT and cyber infrastructure teams.
- **Monitor network activity** for unauthorized communications between SimpleHelp clients and servers.
- **Ensure credentials are secure** and not compromised.
- **Conduct regular security audits and vulnerability assessments** to identify and mitigate risks.

Additional details on mitigation strategy can be found on the Cybersecurity and Infrastructure Security Agency's #StopRansomware page.

## HEALTH-ISAC BULLETIN

"Recent reporting indicates that threat actors are exploiting patched vulnerabilities in SimpleHelp Remote Monitoring and Management (RMM) software to gain unauthorized access to private networks. These vulnerabilities tracked as CVE-2024-57726, CVE-2024-57727, and CVE-2024-57728, were discovered by Horizon3 researchers in late December 2024 and disclosed to SimpleHelp on January 6, prompting the company to release patches. The flaws were publicly disclosed after the patches were released on January 13, 2025.

“This campaign highlights the importance of patch management, as threat actors use exploits within a week of public disclosure.

“The vulnerabilities identified in SimpleHelp RMM could allow attackers to manipulate files and escalate privileges to administrative. A threat actor could chain these vulnerabilities in an attack to gain administrative access to the vulnerable server and then use that access to compromise the device running vulnerable SimpleHelp client software.

“On January 22, approximately a week after the vulnerabilities were disclosed, the cybersecurity firm ArcticWolf identified a malicious campaign running on vulnerable SimpleHelp servers.

“The attack methodology involves the SimpleHelp 'Remote Access[.]exe' process, which was found running on compromised devices, indicating prior installation for remote support. The initial compromise was detected when the SimpleHelp client communicated with an unauthorized server, potentially by exploiting the vulnerabilities or using stolen credentials. Attackers executed commands to gather system intelligence, a precursor to privilege escalation and lateral movement. However, the malicious session was terminated before further actions could be observed.

“While it is not confirmed that the attacks are exploiting these specific vulnerabilities, the timing and nature of the attacks suggest a strong likelihood that the attackers utilized these particular flaws.

“Shadowserver Foundation has reported 580 vulnerable instances of SimpleHelp exposed online, most of which are located in the United States.”

## FURTHER QUESTIONS

If you have further questions, please contact John Riggi, AHA national advisor for cybersecurity and risk, at jriggi@aha.org, or Scott Gee, AHA deputy director for cybersecurity and risk, at sgee@aha.org. For the latest cyber threat intelligence and resources, visit www.aha.org/cybersecurity.

**TLP:CLEAR is a designation to be used when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.*