SimpleHelp RMM Software Leveraged in Exploitation Attempt to Breach Networks

Threat Bulletins	TLP:WHITE	Alert Id: c29d18a1	2025-01-30 20:34:34

Health-ISAC, in collaboration with AHA, has 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 worked with Health-ISAC to ensure this bulletin is distributed widely to the health sector.

It is strongly recommended that all instances of the SimpleHelp application, especially 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 also apply appropriate patches.

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.

Recommendations:

- Immediate Software Update: Users of SimpleHelp RMM software should upgrade to the latest versions (5.5.8, 5.4.10, or 5.3.9) that address the identified vulnerabilities. Detailed instructions for applying these updates are available in SimpleHelp's security bulletin.
- Uninstall Unused Clients: If SimpleHelp clients were previously installed for remote support but are no longer in use, it is recommended that they be uninstalled to reduce the attack surface.
- Monitor Network Activity: Organizations should monitor network traffic for unauthorized communications between SimpleHelp clients and servers, which may indicate a compromise.
- Credential Security: Ensure that credentials used for SimpleHelp are secure and have not been compromised. Consider implementing multi-factor authentication for additional security.

- Regular Security Audits: Conduct regular security audits and vulnerability assessments to identify and mitigate potential risks associated with remote management tools.

Reference(s): archive, Bleeping Computer, fieldeffect, simple-help, arcticwolf, archive
Sources:
https://www.bleepingcomputer.com/news/security/hackers-exploiting-flaws-in-simplehelp-rmm-to-breach-networks/
https://web.archive.org/web/20250115064333/https://www.horizon3.ai/attack-research/disclosures/critical-vulnerabilities-in-simplehelp-remote-support-software/
https://arcticwolf.com/resources/blog-uk/arctic-wolf-observes-campaign-exploiting-simplehelp-rmm-software-initial-access/
https://fieldeffect.com/blog/targeting-of-simplehelp-remote-access-observed
Incident Date: Jan 29, 2025 (UTC)

Tags: CVE-2024-57728, CVE-2024-57727, CVE-2024-57726, SimpleHelp
TLP:WHITE: Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.
Conferences, Webinars, and Summits:
https://h-isac.org/events/
Share Threat Intel:
For guidance on sharing indicators with Health-ISAC via HTIP, please visit the Knowledge Base article "HTIP - Share Threat Intel" here.

The "Share Threat Intel" feature allows for attributed or anonymous sharing across ISACs and other cybersecurity-related entities.
For Questions or Comments:
Please email us at toc@h-isac.org