CYBER ADVISORY

TLP:CLEAR
10 February 2025

Chained Vulnerabilities exploit SimpleHelp RMM Software

SimpleHelp RMM | Sliver Malware | Privilege Escalation | Chained Vulnerabilities

The California Cybersecurity Integration Center (Cal-CSIC) has identified ongoing exploitation of chained vulnerabilities in SimpleHelp Remote Monitoring and Management (RMM) software v5.5.7 and earlier to deploy Sliver malware post-exploitation framework. SimpleHelp offers a Remote Access feature that allows users to access their work or home machines remotely. These vulnerabilities include CVE-2024-57726, CVE-2024-57727, and CVE-2024-57728. Additionally, the Center for Internet Security has released a security advisory warning and technical summary of threat actors leveraging these vulnerabilities in unison in active on-going campaigns[1].

The most significant vulnerability, CVE-2024-55726 has a CVSS 3.1 score of 9.9[2]. The vulnerability is founded on missing authorization checks for certain admin functions, which could be exploited by attackers to escalate their privileges to admin chained with CVE-2024-57728 to take over the server.[3]. The second significant vulnerability, CVE-2024-57727 has a CVSS 3.1 score of 7.5, is an unauthenticated path traversal vulnerability that could allow attackers to download arbitrary files from the SimpleHelp server, including logs and configuration secrets.[4]. The third significant vulnerability in the chain, CVE-2024-57728, has a CVSS 3.1 score of 7.2. It is an arbitrary file upload flaw that can be exploited by authenticated attackers to upload arbitrary files to the machine running the SimpleHelp server or interact with/access remote machines if unattended access option is switched on.[5]

Successful exploitation of these chained vulnerabilities could allow for remote code execution in the context of the system. Depending on the privileges associated with the system, an attacker can install new programs and view, change, or delete data.

Title	CVE (CVSS 3.1)	Description	Affected products
Missing authorization checks for certain admin functions	CVE-2024-57726(9.9)	Allows low-privileges technicians to create API keys with excessive permissions These API keys can be used to escalate privileges to the server admin role	SimpleHelp remote support software v5.5.7 and before
Unauthenticated multiple Path Traversal vulnerabilities	CVE-2024-57727(7.5)	Allows unauthenticated remote attackers to download server configuration files containing various secrets and hashed user passwords from the SimpleHelp host via crafted HTTP requests.	SimpleHelp remote support software v5.5.7 and before
Arbitrary file upload flaw	CVE-2024-57728(7.2)	Allows admin users to upload arbitrary files anywhere on the file system by uploading a zip file. Can be used to execute arbitrary code on the host in the context of the SimpleHelp server user.	SimpleHelp remote support software v5.5.7 and before

The Cal-CSIC recommends immediately applying the appropriate updates provided by SimpleHelp to vulnerable systems.

For more information on applying the security updates please refer to the Security Vulnerabilities in SimpleHelp 5.5.7 and earlier

Organization, Source, Reference, and Dissemination Information

WARNING: This document is the exclusive property of the California Cybersecurity Integration Center (CAL-CSIC) and abides by Traffic Light Protocol (TLP) standards for distribution purposes. It may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 6250, et seq.). Recipients must control, store, handle, transmit, distribute, and dispose of this product in accordance with the TLP standard relating to shared intelligence. Do not release to the public, media, or other personnel who do not have a valid need-to-know without prior approval of an authorized CAL-CSIC official.

Organization Description	California Government Code § 8586.5 established the California Cybersecurity Integration Center (Cal-CSIC) as the central organizing hub of state government's cybersecurity activities, including information sharing, intelligence analysis, incident response, and overarching cybersecurity strategy. The Cal-CSIC is responsible for reducing the likelihood and severity of cyber incidents that could damage California's economy, critical infrastructure, and public or private sector networks in our state.
Customer Feedback	If you need further information about this issue, contact the Cal-CSIC at our email address CalCSIC@caloes.ca.gov or by telephone at (833) REPORT1. To help us identify ways to better assist you, please submit feedback here.
Source Summary Statement	This report was compiled from a variety of sources, predominately open-source reporting.
Handling Caveats	**Traffic Light Protocol (TLP):** Recipients may share TLP:CLEAR information with the world; there is no limit on disclosure. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

[1] Center for Internet Security; "Multiple Vulnerabilities in SimpleHelp RMM Could Allow for Arbitrary Code Execution; Multiple Vulnerabilities in SimpleHelp RMM Could Allow for Arbitrary Code Execution; accessed 10 February 2025.

[2] National Vulnerability Database; "CVE-2024-55726 Detail"; https://nvd.nist.gov/vuln/detail/CVE-2024-57726; accessed 10 February 2025.

[3] Center for Internet Security; "Multiple Vulnerabilities in SimpleHelp RMM Could Allow for Arbitrary Code Execution; Multiple Vulnerabilities in SimpleHelp RMM Could Allow for Arbitrary Code Execution; accessed 10 February 2025

[4] National Vulnerability Database; "CVE-2024-57727 Detail"; https://nvd.nist.gov/vuln/detail/CVE-2024-57727; accessed 10 February 2025.

[5] National Vulnerability Database; "CVE-2024-57728 Detail"; https://nvd.nist.gov/vuln/detail/CVE-2024-57728; accessed 10 February 2025.

CAL-CSIC-202502-002

WARNING: This document is the exclusive property of the California Cybersecurity Integration Center (CAL-CSIC) and abides by Traffic Light Protocol (TLP) standards for distribution purposes. It may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 6250, et seq.). Recipients must control, store, handle, transmit, distribute, and dispose of this product in accordance with the TLP standard relating to shared intelligence. Do not release to the public, media, or other personnel who do not have a valid need-to-know without prior approval of an authorized CAL-CSIC official.

TLP:CLEAR

3