CYBER ADVISORY

TLP:CLEAR
11 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. The most significant vulnerability, CVE-2024-55726 has a CVSS 3.1 score of 9.9[1] and is chained to CVE-2024-7727 and CVE-2024-57728. The vulnerability is founded on missing authorization checks for certain admin functions. 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.[2]

Title	CVE (CVSS 3.1)	Description	Affected products
Missing authorization checks for certain admin functions	CVE-2024-57726(9.9)	Allows low-privilege 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 users 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

Table 1

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

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.
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] National Vulnerability Database; "CVE-2024-55726 Detail"; https://nvd.nist.gov/vuln/detail/CVE-2024-57726; accessed 10 February 2025.
[2] Center for Internet Security; "Multiple Vulnerabilities in SimpleHelp RMM Could Allow for Arbitrary Code Execution"; https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-simplehelp-rmm-could-allow-for-arbitrary-code-execution_2025-012; accessed 10 February 2025.