مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Multiple Vulnerabilities in SimpleHelp RMM

Tracking #:432316811

Date:31-01-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed several critical vulnerabilities have been discovered in SimpleHelp RMM (Remote Monitoring and Management), a widely used remote access software.

TECHNICAL DETAILS:

Multiple vulnerabilities have been discovered in SimpleHelp RMM that could allow for arbitrary code execution. The most severe vulnerabilities, when chained together, could enable attackers to gain full control over the affected system, potentially installing malicious programs, accessing or altering sensitive data, or deleting files.

Vulnerability Details:

- CVE-2024-57727-Unauthenticated Path Traversal Vulnerability: This flaw allows attackers to download arbitrary files from the SimpleHelp server, including sensitive logs and configuration secrets. The configuration secrets are encrypted with a hardcoded key, but could still provide attackers with valuable information.
- CVE-2024-57728-Arbitrary File Upload Vulnerability: Authenticated attackers (potentially using stolen admin credentials) can upload arbitrary files to the server running SimpleHelp. If the server is configured for unattended access, this could allow attackers to access remote machines. For Linux servers, the vulnerability could be exploited to upload a crontab file, executing remote commands. On Windows servers, an attacker could overwrite critical executable files or libraries used by SimpleHelp, enabling remote code execution.
- CVE-2024-57726-Missing Authorization Checks for Admin Functions: This vulnerability allows attackers to bypass authorization checks for certain admin functions, potentially escalating their privileges to admin level. This would make it easier for attackers to exploit CVE-2024-57728 and take full control over the server.

Systems Affected:

- SimpleHelp v5.5
- SimpleHelp v5.4
- SimpleHelp v5.3

Fixed Versions:

- SimpleHelp 5.5.8 or Patches v5.4.10 or 5.3.9

RECOMMENDATIONS:

- Users of SimpleHelp RMM should immediately update to the latest patched version of the software.
- Limit access to the SimpleHelp server to only authorized users, and ensure that admin-level privileges are granted only when necessary. This reduces the risk of exploitation through compromised admin credentials.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://www.helpnetsecurity.com/2025/01/16/critical-simplehelp-vulnerabilities-fixed-security-update-remote-support/