مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Actively Exploited Critical Vulnerabilities in SimpleHelp Remote Support

Tracking #:432318842

Date:26-04-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that multiple critical vulnerabilities have been identified in SimpleHelp Remote Support Software, a remote access tool used for IT support and unattended remote management.

TECHNICAL DETAILS:

Multiple critical vulnerabilities have been identified in SimpleHelp Remote Support Software, a remote access tool used for IT support and unattended remote management. These flaws enable attackers to access sensitive configuration data, escalate privileges, and achieve full remote code execution (RCE) on affected servers and potentially connected client systems.

Exploited Vulnerability Details:

1. CVE-2024-57726 – Privilege Escalation (Technician → Admin)
   - Severity: Critical (CVSS 9.9)
   - Attack Vector: Authenticated (Low-privilege technician)
   - Enables chaining with CVE-2024-57728 for complete compromise
2. CVE-2024-57728 – Arbitrary File Upload → Remote Code Execution
   - Severity: High (CVSS 7.2)
   - Attack Vector: Authenticated (Admin or privileged technician)

Critical Vulnerability:

3. CVE-2024-57727- Unauthenticated Path Traversal
   - Severity: 9.1 Critical
   - Allows attackers to download arbitrary files from the server without authentication.
   - Exploits improper input validation leading to path traversal

Fixed Versions:

- 5.5.8 / 5.4.10 / 5.3.9 or later

RECOMMENDATIONS:

- Upgrade SimpleHelp Remote Support Software immediately to the fixed version.

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://guides.simple-help.com/kb---security-vulnerabilities-01-2025#remote-machine-compromise