مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Actively Exploited Critical Vulnerability in SimpleHelp

Tracking #:432319216

Date:30-06-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical authentication bypass vulnerability, CVE-2026-48558 (CVSS 10.0), has been identified in SimpleHelp, a widely used Remote Monitoring and Management (RMM) solution.

TECHNICAL DETAILS:

A critical authentication bypass vulnerability, CVE-2026-48558 (CVSS 10.0), has been identified in SimpleHelp, a widely used Remote Monitoring and Management (RMM) solution. The vulnerability affects SimpleHelp servers configured to use OpenID Connect (OIDC) authentication and allows an unauthenticated attacker to bypass authentication by submitting forged identity tokens.
The vulnerability is being actively exploited in the wild and have been observed exploiting the flaw to gain technician-level access, deploy the TaskWeaver Node.js malware loader, and install Djinn Stealer to steal credentials, cloud access keys, browser data, cryptocurrency wallets, and AI development tokens.
Organizations using affected SimpleHelp versions should immediately upgrade to the latest patched release and investigate systems for signs of compromise.

Vulnerability Details:

- CVE ID: CVE-2026-48558
- CVSS 3.1 Score: 10.0 (Critical)
- Product: SimpleHelp
- Affected Versions
  - 5.5.15 and earlier
  - All 6.0 pre-release versions (configured with OIDC authentication)
- Patched Versions
  - 5.5.16
  - 6.0 RC2

RECOMMENDATIONS:

Immediate Actions:

- Organizations should treat it as an emergency. Immediate patching, credential rotation, and a thorough compromise assessment are essential to prevent unauthorized access and malware deployment across managed environments.

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://simple-help.com/security/simplehelp-security-update-2026-05