AUTORITETI KOMBËTAR

PËR SIGURINË KIBERNETIKE

Dobësitë kritike të shfrytëzuara në mënyrë aktive në SimpleHelp Remote Support

Data: 27/04/2026
Version: 1.0

Përmbajtja

Përmbledhje Ekzekutive

Janë identifikuar disa dobësi kritike në SimpleHelp Remote Support Software, një mjet qasjeje në distancë që përdoret për mbështetje IT dhe menaxhim në distancë pa mbikëqyrje.

Informacione Teknike

Janë identifikuar disa dobësi kritike në SimpleHelp Remote Support Software, një mjet për akses në distancë që përdoret për mbështetje IT dhe menaxhim në distancë pa mbikëqyrje. Këto dobësi u mundësojnë sulmuesve të hyjnë në të dhëna sensitive konfigurimi, të përshkallëzojnë privilegjet dhe të arrijnë ekzekutim të plotë të kodit në distancë (RCE) në serverat e prekur dhe sistemet e klientëve potencialisht të lidhur.

Detajet e Dobësisë së Shfrytëzuar:
1. CVE-2024-57726 – Përshkallëzim i Privilegjit (Teknik → Administrator)
• Ashpërsia: Kritike (CVSS 9.9)
• Vektori i Sulmit: I Autentifikuar (Teknik me privilegje të ulëta)
• Mundëson lidhjen zinxhir me CVE-2024-57728 për kompromentim të plotë
2. CVE-2024-57728 – Ngarkim Arbitrar i Skedarit → Ekzekutim i Kodit në Distancë
• Ashpërsia: E Lartë (CVSS 7.2)
• Vektori i Sulmit: I Autentifikuar (Administrator ose teknik i privilegjuar)
Dobësi Kritike:
3. CVE-2024-57727- Kalim path i Paautorizuar
• Ashpërsia: 9.1 Kritike
• Lejon sulmuesit të shkarkojnë skedarë arbitrarë nga serveri pa autentifikim.
• Shfrytëzon validimin e papërshtatshëm të të dhënave hyrëse që çon në përshkimin e shtegut
Versionet e përditësuar:
• 5.5.8 / 5.4.10 / 5.3.9 ose më të reja

Rekomandime

AKSK rekomandon te përmirësoni programin e SimpleHelp Remote Support versionin e përditësuar.