INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-16 08:12 UTC

SimpleHelp CVE-2026-48558: Unauthenticated Account Creation Exposes ~1,000 Enterprise RMM Servers

CVE VULNERABILITY | **CRITICAL** | CVSS 9.5

SCC Item ID	SCC-CVE-2026-0309
Type	CVE Vulnerability
CVE ID	CVE-2026-48558
Severity	CRITICAL
CVSS Base Score	9.5
EPSS Score	0.0063 (45th percentile)
Affected Products	SimpleHelp versions 5.5.15 and older; SimpleHelp 6.0 pre-release versions with OIDC authentication enabled
Published	2026-06-15T16:06:52
Discovery Source	Rss

Executive Summary

A critical authentication bypass in SimpleHelp RMM software (CVE-2026-48558, CVSS 9.5) allows unauthenticated attackers to create privileged administrator accounts on exposed servers, bypassing multi-factor authentication entirely. Approximately 1,000 internet-exposed SimpleHelp servers are vulnerable today, with patches available as of June 9, 2026. Because RMM tools provide deep, trusted access to all managed endpoints, a successful compromise gives attackers a direct path to every device under that server's management, representing severe enterprise-wide exposure.

Technical Analysis

CVE-2026-48558 is a critical authentication bypass in SimpleHelp RMM affecting versions 5.5.15 and earlier and 6.0 pre-release builds with OIDC authentication enabled. The vulnerability resides in the OIDC authentication flow and permits unauthenticated remote attackers to register Technician-level accounts directly, circumventing credential validation and MFA. Assigned CWEs: CWE-287 (Improper Authentication), CWE-306 (Missing Authentication for Critical Function), CWE-284 (Improper Access Control). CVSS base score: 9.5 (Critical). Mapped MITRE ATT&CK techniques include T1190 (Exploit Public-Facing Application), T1078 (Valid Accounts), T1078.003 (Local Accounts), T1078.004 (Cloud Accounts), T1021.001 (Remote Desktop Protocol), T1059 (Command and Scripting Interpreter), and T1133 (External Remote Services). Exploitation requires

OIDC authentication to be configured on the target; of an estimated 14,000 internet-exposed SimpleHelp servers, approximately 1,000 are believed to meet this condition. Patches were released June 9, 2026. SimpleHelp has a documented prior exploitation history by ransomware groups and nation-state-affiliated operators. Sources: NVD (nvd.nist.gov/vuln/detail/CVE-2026-48558), CVE Record (cve.org), Horizon3.ai disclosure, BleepingComputer.

Action Checklist

1. Step 1: Containment, Immediately restrict internet access to all SimpleHelp server management interfaces. Identify every instance running version 5.5.15 or earlier, or any 6.0 pre-release build. If OIDC authentication is enabled on any instance, treat it as potentially compromised and isolate it from managed endpoints until patched. Block inbound access to SimpleHelp ports from untrusted networks at the perimeter firewall (NIST AC-17; CIS 4.4).
2. Step 2: Detection, Audit all SimpleHelp Technician accounts for unrecognized entries, especially accounts created after the patch window opened (June 9, 2026). Review SimpleHelp server logs for account creation events originating from unauthenticated or anomalous sources. Examine authentication logs for OIDC flow activity from unexpected IP ranges. Apply IOCs published by Horizon3.ai (see Sources section) to firewall, SIEM, and EDR platforms. Reference NIST AU-2, AU-6, AU-12 for event logging and audit review requirements.
3. Step 3: Eradication, Apply the official SimpleHelp patch released June 9, 2026, upgrading all instances to a patched version above 5.5.15 (or the patched 6.0 release). If immediate patching is not possible, disable OIDC authentication on all exposed servers as a temporary mitigation. After patching, audit and remove any Technician accounts not created through authorized processes. Rotate all Technician and administrator credentials (NIST AC-2; D3-CRO Credential Rotation; D3-CH Credential Hardening; CIS 5.2).
4. Step 4: Recovery, After patching, re-enable managed endpoint connectivity in a staged manner, verifying server integrity before restoring full access. Confirm OIDC authentication configuration is clean and no rogue identity provider entries exist. Enable enhanced audit logging on account creation and authentication events for a minimum 30-day monitoring period post-remediation (NIST AU-6, AU-9; CIS 8.2). Validate that MFA enforcement is functioning correctly for all Technician accounts (D3-MFA; CIS 6.5).
5. Step 5: Post-Incident, Document the gap between patch release (June 9, 2026) and your remediation date as a metric for patch velocity improvement. Review RMM tool exposure policy: assess whether SimpleHelp management interfaces require internet exposure or whether VPN-gated access is feasible (NIST AC-17; CIS 6.4). Conduct a broader RMM software inventory to identify any similar OIDC or SSO configurations across other tools. Given SimpleHelp's prior exploitation history by ransomware and nation-state actors, elevate RMM infrastructure to a high-value target tier in your threat model (NIST AC-6; D3-UAP User Account Permissions).

Detection Guidance

Primary detection focus: unauthorized Technician account creation via the OIDC authentication endpoint. Query SimpleHelp server logs for account registration events where the originating session has no prior authenticated state. Look for HTTP requests to OIDC callback or account creation endpoints arriving without a valid session

token or from IPs not associated with known identity providers. Cross-reference new Technician accounts against your authorized account inventory (CIS 5.1). In your SIEM, alert on SimpleHelp account creation events outside of approved change windows. Apply IOCs published by Horizon3.ai (see Sources section) to identify known exploitation infrastructure. Behavioral indicators post-exploitation include unexpected remote sessions initiated from newly created Technician accounts, lateral movement from managed endpoints (T1021.001), and script execution via RMM console (T1059). Monitor for new scheduled tasks, service installations, or persistence mechanisms on managed endpoints following any suspicious RMM session. NIST AU-6 and AU-12 govern audit review and generation requirements. CIS 8.2 requires audit log collection across enterprise assets.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`https://horizon3.ai/attack-research/disclosures/cve-2026-48558-simplehelp-authentication-bypass-iocs/`	Horizon3.ai published IOC list specific to CVE-2026-48558 exploitation activity — check this source for current IP and infrastructure indicators	HIGH

Framework Mappings

MITRE-ATTACK

- **T1021.001** — Remote Desktop Protocol
- **T1078.003** — Local Accounts
- **T1078.004** — Cloud Accounts
- **T1059** — Command and Scripting Interpreter
- **T1190** — Exploit Public-Facing Application
- **T1133** — External Remote Services
- **T1078** — Valid Accounts

NIST-800-53R5

- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-7** — Software, Firmware, and Information Integrity
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **AC-17** — Remote Access
- **AC-20** — Use of External Systems
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **AC-3** — Access Enforcement
- **IA-8** — Identification and Authentication (Non-Organizational Users)
- **CP-9** — System Backup
- **IR-4** — Incident Handling

OWASP-TOP10-2021

- **A01:2021** — Broken Access Control
- **A07:2021** — Identification and Authentication Failures

CIS-V8

- **6.1** — Establish an Access Granting Process
- **6.2** — Establish an Access Revoking Process
- **6.3** — Require MFA for Externally-Exposed Applications
- **6.4** — Require MFA for Remote Network Access
- **6.5** — Require MFA for Administrative Access
- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management
- **8.2** — Collect Audit Logs

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets

HIPAA-SECURITY

- **164.312(a)(1)** — Access Control
- **164.312(d)** — Person or Entity Authentication
- **164.308(a)(7)(ii)(A)** — Data Backup Plan

NIST-CSF-2

- **RS.MI-01** — Incidents are contained
- **DE.CM-01** — Networks and network services are monitored

ISO-27001-2022

- **A.5.29** — Information security during disruption
- **A.8.8** — Management of technical vulnerabilities

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1021.001	Remote Desktop Protocol	Lateral-Movement

Technique ID	Technique Name	Tactic
T1078.003	Local Accounts	Defense-Evasion
T1078.004	Cloud Accounts	Defense-Evasion
T1059	Command and Scripting Interpreter	Execution
T1190	Exploit Public-Facing Application	Initial-Access
T1133	External Remote Services	Persistence
T1078	Valid Accounts	Defense-Evasion

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/simplehelp-bug-lets-...	T3
CVE-2026-48558: SimpleHelp Auth Bypass IOCs | Horizon3.ai	https://horizon3.ai/attack-research/disclosures/cve-2026-48558-simp...	T3
CVE-2026-48558 - CVE Record	https://www.cve.org/CVERecord?id=CVE-2026-48558	T3
CVE-2026-48558 - Exploits & Severity - Feedly	https://feedly.com/cve/CVE-2026-48558	T3
NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-48558	T1

Generated 2026-06-16 08:12 UTC by TJS Security Command Center