CYBER ADVISORY

Monday, June 15, 2026 **CAL-CSIC-202606-A-011**

Maximum-Severity Vulnerability Impacting SimpleHelp Remote Support Software

Remote Code Execution	Unauthenticated Attacker	Full Administrative Control	Patch Available

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of a critical vulnerability impacting SimpleHelp's Remote Support Software. CVE-2026-48558 carries a 3.1 CVSS score of 10.0.[1] The vulnerability is rooted in the Open ID Connect (OIDC) authentication process. When OIDC is configured, the system fails to verify the cryptographic signature of the identity tokens submitted during a login. CVE-2026-48558 enables an unauthenticated, remote attacker to create a forged token containing arbitrary identity claims to gain a fully authenticated technician session. Certain configurations of OIDC would also permit multi-factor authentication bypass. No user interaction is required.

Certain conditions have to be met for an attacker to exploit as a technician.

1. OIDC is enabled
2. At least one "TechnicianGroup" has the OIDC provider enabled for it
3. "Allow group authenticated logins" is enabled on the TechnicianGroup

Successful exploitation would allow the attacker to impersonate as a technician to perform privileged management activities such as remoting into managed endpoints and executing scripts to gain full administrative control over the targeted system.[2]

SimpleHelp has issued a security update for CVE-2026-48558. The Cal-CSIC recommends following SimpleHelp's patching guidance as soon as possible.[3] If patching is not immediately possible, restrict technician login sources using IP-based allowlists. For additional vulnerability details and IOC hunting regarding CVE-2026-48558 please use this link:

IOC Details: https://horizon3.ai/attack-research/disclosures/cve-2026-48558-simplehelp-authentication-bypass-iocs/

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

Affected Product(s) and Version(s)

Product	Affected Version
SimpleHelp	5.5.0, 6.0

Cal-CSIC services are provided at no cost to assist organizations in strengthening their cybersecurity defenses. If you need assistance or wish to verify this communication, please contact us at (833) REPORT-1, or (916) 636-2997. Visit our website for more details: California Cybersecurity Integration Center | California Governor's Office of Emergency Services

References

[1] OpenCVE; "CVE-2026-48558- SimpleHelp Authentication Bypass via Missing OIDC JWT Signature Verification"; https://app.opencve.io/cve/CVE-2026-48558; accessed 15 June 2026
[2] Horizon3.ai; "CVE-2026-48558: SimpleHelp Authentication Bypass Indicators of Compromise"; https://horizon3.ai/attack-research/disclosures/cve-2026-48558-simplehelp-authentication-bypass-iocs/; accessed 15 June 2026
[3] SimpleHelp; "SimpleHelp 5.5 and 6.0 Security Fix"; https://simple-help.com/security/simplehelp-security-update-2026-05; accessed 15 June 2026