SOCFortress CoPilot: Hardcoded JWT secret allows unauthenticated full admin compromise and lateral movement into all integrated SOC tools

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-42869
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-11 20:25:43 UTC
Updated	2026-05-12 14:17:05 UTC
Description	SOCFortress CoPilot focuses on providing a single pane of glass for all your security operations needs. Prior to 0.1.57, SO

Risk And Classification

Primary CVSS: v3.1 10 CRITICAL from security-advisories@github.com

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

EPSS: 0.001190000 probability, percentile 0.303350000 (date 2026-05-12)

Problem Types: CWE-287 | CWE-522 | CWE-798 | CWE-287 CWE-287: Improper Authentication | CWE-522 CWE-522: Insufficiently Protected Credentials | CWE-798 CWE-798: Use of Hard-coded Credentials

Version	Source	Type	Score	Severity	Vector
3.1	security-advisories@github.com	Secondary	10	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
3.1	CNA	DECLARED	10	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Changed

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Socfortress	CoPilot	affected < 0.1.57	Not specified

References

Reference	Source	Link
github.com/socfortress/CoPilot/commit/4640511a0cf2e7b144a71375b5b349a831...	security-advisories@github.com	github.com
github.com/socfortress/CoPilot/security/advisories/GHSA-4gxj-hw3c-3x2x	134c704f-9b21-4f2e-91b3-4a467353bcc0	github.com
github.com/socfortress/CoPilot/pull/814	security-advisories@github.com	github.com
CVE Program record	CVE.ORG	www.cve.or
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© CVE.report 2026 |
Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**