



FreshRSS has an authentication bypass due to truncated bcrypt hash [edge branch]

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2025-68402
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-09 20:16:01 UTC
Updated	2026-04-28 21:11:07 UTC
Description	FreshRSS is a free, self-hostable RSS aggregator. From 57e1a37 - 00f2f04, the lengths of the nonce was changed from 40

Risk And Classification

Primary CVSS: v4.0 8.2 HIGH from security-advisories@github.com

CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

EPSS: 0.000590000 probability, percentile 0.182610000 (date 2026-04-28)

Problem Types: CWE-287 | CWE-287 CWE-287: Improper Authentication

Version	Source	Type	Score	Severity	Vector
4.0	security-advisories@github.com	Secondary	8.2	HIGH	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X
4.0	CNA	DECLARED	8.2	HIGH	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

High

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

Confidentiality

High

Integrity

None

Availability

None

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	FreshRSS	FreshRSS	affected < 476e57b04646416e24e24c56133c9fadf9e52b95	Not specified

References

Reference	Source	Link	T
github.com/FreshRSS/FreshRSS/pull/8320	security-advisories@github.com	github.com	
github.com/FreshRSS/FreshRSS/commit/476e57b04646416e24e24c56133c9fadf9e5...	security-advisories@github.com	github.com	
github.com/FreshRSS/FreshRSS/security/advisories/GHSA-pcq9-mq6m-mvmp	security-advisories@github.com	github.com	
github.com/FreshRSS/FreshRSS/pull/8061	security-advisories@github.com	github.com	
CVE Program record	CVE.ORG	www.cve.org	c
NVD vulnerability detail	NVD	nvd.nist.gov	c

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 registered 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

