Sonarr Authentication Bypass vulnerability

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2026-30975
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-25 21:16:41 UTC
Updated	2026-03-30 16:55:47 UTC
Description	Sonarr is a PVR for Usenet and BitTorrent users. Versions prior to 4.0.16.2942 have an authentication bypass that affected

Risk And Classification

Primary CVSS: v3.1 9.8 CRITICAL from nvd@nist.gov

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

EPSS: 0.000650000 probability, percentile 0.201070000 (date 2026-04-01)

Problem Types: CWE-290 | CWE-290 CWE-290: Authentication Bypass by Spoofing

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	security-advisories@github.com	Secondary	8.1	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N
3.1	CNA	DECLARED	8.1	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

ntegrity

High

Availability

High

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sonarr	Sonarr	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Sonarr	Sonarr	affected < 4.0.16.2942	Not specified

References

Reference	Source	Link	Tags
github.com/Sonarr/Sonarr/releases/tag/v4.0.16.2942	security-advisories@github.com	github.com	Release Notes
github.com/Sonarr/Sonarr/releases/tag/v4.0.16.2944	security-advisories@github.com	github.com	Release Notes
github.com/Sonarr/Sonarr/security/advisories/GHSA-h5qx-5hjf-7c9r	security-advisories@github.com	github.com	Vendor Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

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.

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