

NEW

The AI-powered identity future: Where strategy meets execution. May 19-21. [Register now](#) →

# SailPoint IdentityIQ Role Editor Incorrect Authorization Vulnerability – CVE-2026-5712

## Description

This vulnerability impacts all versions of IdentityIQ and allows an authenticated identity that is the requestor or assignee of a work item to edit the definition of a role without having an assigned capability that would allow role editing.

## Affected product and versions

- IdentityIQ 8.5 and all 8.5 patch levels prior to 8.5p2
- IdentityIQ 8.4 and all 8.4 patch levels prior to 8.4p4
- IdentityIQ 8.3 and all 8.3 patch levels prior to 8.3p5
- All previous versions are affected

# Resolution

SailPoint has released [IIQSR-972](#) for each impacted and supported version of IdentityIQ. Future patch levels will include the fixes once they become available.

## CVE details

**CVE ID:** CVE-2026-5712

**Published Date:** 04/29/2026

**Vulnerability Type:** IdentityIQ Role Editor Incorrect Authorization Vulnerability

**CWE:** CWE-863

**CVSS v3 Score:** 8.0

**CVSS v3 Vector:** CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:C/C:H/I:H/A:H

## References

[IdentityIQ Role Editor Incorrect Authorization Vulnerability – IIQSR-972.](#)



### PRODUCTS

- Platform
- Identity Security Cloud
- Compare suites
- IdentityIQ

### SERVICES

- Support portal ↗
- Documentation ↗
- Developer forum ↗
- Training & certification

[Connectors & Integrations](#)

[Professional services](#)

[Contact us](#)

**RESOURCES**

**COMPANY**

[Resource library](#)

[About us](#)

[Blog](#)

[Why us](#)

[Podcasts](#)

[Why work at SailPoint](#)

[Events](#)

[News center](#)

[Webinars](#)

[Trust center](#)

[Partners](#)

[Leadership team](#)

[Glossary](#)

[Investor relations ↗](#)

[Environmental, Social, and Governance ↗](#)

---

[Terms of use](#) [Legal](#) [Privacy policy](#) [Cookie notice](#) [Don't Sell/Share My Data !\[\]\(1ed10657a19f9137278430c48fd18626\_img.jpg\)](#)

[Email preferences](#) [Disclosure policy](#)

© 2026 SailPoint Technologies, Inc. All Rights Reserved.