IdentityIQ Role Editor Incorrect Authorization Vulnerability

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

Summary

CVE	CVE-2026-5712
State	PUBLISHED
Assigner	SailPoint
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-29 18:16:05 UTC
Updated	2026-04-30 15:48:26 UTC
Description	This vulnerability impacts all versions of IdentityIQ and allows an authenticated identity that is the requestor or assignee of a

Risk And Classification

Primary CVSS: v3.1 8 HIGH from psirt@sailpoint.com

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

EPSS: 0.000360000 probability, percentile 0.105190000 (date 2026-05-02)

Problem Types: CWE-863 | CWE-863 CWE-863: Incorrect Authorization

Version	Source	Type	Score	Severity	Vector
3.1	psirt@sailpoint.com	Secondary	8	HIGH	CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:C/C:H/I:H/A:H
3.1	CNA	CVSS	8	HIGH	CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:C/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

Low

User Interaction

Required

Scope

Changed

Confidentiality

High

ntegrity

High

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	SailPoint Technologies	IdentityIQ	affected 8.5 8.5p2 custom	Not specified
CNA	SailPoint Technologies	IdentityIQ	affected 8.4 8.4p4 custom	Not specified
CNA	SailPoint Technologies	IdentityIQ	affected 8.3 8.3p5 custom	Not specified

References

Reference	Source	Link	Tags
www.sailpoint.com/security-advisories/sailpoint-identityiq-role-editor-incorrec...	psirt@sailpoint.com	www.sailpoint.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analys

Vendor Comments And Credit

Discovery Credit

CNA: wildwildwes (en)

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