Cisco Intersight Device Connector for Nutanix Prism Central Unauthenticated API Access

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

Summary

CVE	CVE-2026-5944
State	PUBLISHED
Assigner	Nutanix
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-28 14:16:13 UTC
Updated	2026-04-28 20:23:20 UTC
Description	An improper access control vulnerability exists in the Cisco Intersight Device Connector for Nutanix Prism Central. The serv

Risk And Classification

Primary CVSS: v4.0 6.7 MEDIUM from 2ffdacf6-8681-47df-b023-4f11abd61c1d

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

Problem Types: CWE-306 | CWE-862 | CWE-306 CWE-306 Missing authentication for critical function | CWE-862 CWE-862 Missing Authorization

Version	Source	Type	Score	Severity	Vector
4.0	2ffdacf6-8681-47df-b023-4f11abd61c1d	Secondary	6.7	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:H/
4.0	CNA	CVSS	6.7	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:H/
3.1	2ffdacf6-8681-47df-b023-4f11abd61c1d	Secondary	8.2	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H
3.1	CNA	CVSS	8.2	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H
2.0	2ffdacf6-8681-47df-b023-4f11abd61c1d	Secondary	8.5		AV:N/AC:L/Au:N/C:P/I:N/A:C
2.0	CNA	CVSS	8.5		AV:N/AC:L/Au:N/C:P/I:N/A:C

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

Low

Integrity

None

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

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

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

None

Availability

High

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

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

None

Availability

Complete

AV:N/AC:L/Au:N/C:P/I:N/A:C

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Nutanix	Cisco Intersight Device Connector For Prism Central	affected 4.3.0 7.5.1 custom	Not specified

References

Reference	Source	Link	Tags
portal.nutanix.com/page/documents/list	2ffdacf6-8681-47df-b023-4f11abd61c1d	portal.nutanix.com	
www.nutanix.com/support	2ffdacf6-8681-47df-b023-4f11abd61c1d	www.nutanix.com	
download.nutanix.com/alerts/Security_Advisory_0046.pdf	2ffdacf6-8681-47df-b023-4f11abd61c1d	download.nutanix.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, ana

Vendor Comments And Credit

Discovery Credit

CNA: External Security Researcher (via Cisco) (en)

Additional Advisory Data

Source	Time	Event
CNA	2026-04-08T15:45:00.000Z	Initial vulnerability analysis and internal update
CNA	2026-04-08T18:30:00.000Z	CVE reserved
CNA	2026-04-28T13:06:00.000Z	Advisory published

Solutions

CNA: Nutanix has released version 7.5.1 of the Cisco Intersight Device Connector: * Log in to Prism Central (PC) and navigate to the Life Cycle Manager (LCM) Dashboard. * Click "Perform Inventory" or "Get Full Inventory" to refresh the inventory. * After the inventory

"Perform Inventory" or "Get Full Inventory" to refresh the inventory." After the inventory refresh completes, navigate to the Marketplace. * Select the Cisco Intersight Device Connector. * Click "Upgrade" to update to version 7.5.1 or later.

Workarounds

CNA: If upgrading the Cisco Intersight Device Connector to version 7.5.1 or later is not immediately possible, restrict access to TCP port 7373 by limiting the service to internal traffic only: * Establish an SSH session to Prism Central (PC). * Execute the following command to reconfigure the service visibility to internal traffic only: sudo kubectl -n pc-platform-other annotate service cisco-device-connector service.msp.ntnx.io/lb=pc-internal --overwrite * Run the following command: sudo kubectl get svc -n pc-platform-other and verify that the Cisco Intersight Device Connector is no longer associated with the Prism Central public IP address.

Exploits

CNA: The Nutanix Product Security Incident Response Team (PSIRT) is not aware of any public announcements or malicious use of the vulnerability that is described in this advisory.

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