

# Evaluate SNA Vulnerabilities with CVR

## Contents

---

[Introduction](#)

[Looking Up a Vulnerability](#)

[Next Steps](#)

---

## Introduction

This document describes how to use the Cisco Vulnerability Repository (CVR) to evaluate Secure Network Analytics (SNA) vulnerabilities.

## Looking Up a Vulnerability

Cisco enables you to self-serve vulnerability look-ups of Cisco products and to request evaluation of vulnerabilities that have not yet been examined. Cisco needs CVE numbers to evaluate vulnerabilities against our products.

To do this:

1. Navigate to the CVR Website (<https://sec.cloudapps.cisco.com/security/center/cvr>)
2. Enter the CVE number
3. Click the expanding arrow next to 'Narrow Search by Product' so that it is pointing down
4. In the 'Cisco Products' section select 'Cisco Secure Network Analytics'
5. In the 'Cisco Platforms' section select the appropriate device type
6. In the 'Release' section select the appropriate version
7. Click 'Search'
8. The disposition reply is displayed after the search is submitted
9. You can find additional details to that disposition including links to relevant Cisco Defect and Enhancement Tracking System (CDETS) or the CVSS Base Score

Search by CVE 2 Q CVE-2022-43680 7 Search

▼ Narrow search by product 3

Cisco Products

Stealthwatch 4

Cisco Secure Network Analytics

Cisco Platforms

Filter by Platform Name 5

Cisco Stealthwatch Data Store  
Cisco Stealthwatch Flow Collector Series  
Cisco Stealthwatch Flow Sensor Series  
**Cisco Stealthwatch Management Console**  
Cisco Stealthwatch UDP Director

Release

Filter by Release 6

7.5.0 7

7.5.1\_M2M  
7.4.2  
7.4.1  
7.4.0  
7.3.2  
...

Cisco Secure Network Analytics / Cisco Stealthwatch Management Console / 7.5.0 is not impacted by CVE-2022-43680. 8 VEX

Cisco Bugs: N/A

Vulnerability details:

CVSS Base Score: 7.5 9

Vulnerability Description: In libexpat through 2.4.9, there is a use-after free caused by overeager destruction of a shared DTD in XML\_ExternalEntityParserCreate in out-of-memory situations.

The Cisco Vulnerability Repository (CVR) is a vulnerability search engine for CVEs that may impact Cisco products. CVR can help customers understand if their Cisco product is affected by a particular third-party software vulnerability. This tool provides vulnerability disposition information for CVEs reported after 2017, as well as other select CVEs that Cisco has determined to be high risk and any vulnerabilities listed in the Known Exploited Vulnerability (KEV) catalog of the U.S. Cybersecurity & Infrastructure Security Agency (CISA). CVR does not currently include vulnerability disposition information for Cisco cloud offers.

CVR disposition information is available for download in the Vulnerability Exploitability eXchange (VEX) format, and the tool also displays any associated Cisco Security Advisories. For more information about VEX and how to use this tool, see the Frequently Asked Questions page [here](#). For help with a product not listed in this tool, please use the Feedback link on this page or contact your support organization.

The information on this page is provided on an 'as is' basis and does not imply any kind of guarantee or warranty. Cisco reserves the right to change or update this page without notice, and your use of the information or linked materials is at your own risk. Customers whose Cisco products are provided or maintained through prior or existing agreements with third-party support organizations, such as Cisco Partners, authorized resellers, or service providers, should contact that support organization for guidance and assistance with the appropriate course of action in regards to any information provided through this tool.

## Next Steps

### Not Impacted

The SNA version has been evaluated as Not Vulnerable to the bug

Cisco Secure Network Analytics / Cisco Stealthwatch Management Console / 7.5.0 is not impacted by CVE-2022-43680. 8 VEX

Cisco Bugs: N/A

Vulnerability details:

CVSS Base Score: 4.3

Vulnerability Description: IBM Navigator for i 7.3, 7.4, and 7.5 could allow an authenticated user to obtain sensitive information they are authorized to but not while using this interface. By performing an SQL injection an attacker could see user profile attributes through this interface. IBM X-Force ID: 239305.

### Disposition Data is Unavailable

The SNA version has not be evaluated against this vulnerability.

CVE-2022-43680 disposition data is unavailable for Cisco Secure Network Analytics / Cisco Stealthwatch Management Console / 7.3.0. To request a disposition assessment, click the Request Assessment button below.

Request Assessment

### Request Assessment

Click the 'Request Assessment' link to begin the evaluation process. Enter additional comments in the popup and hit the "Submit" button to submit the bug to the Cisco PSIRT team for evaluation. Once submitted, the bug changes to "Disposition Data Request Submitted".

Request CVE-2022-43680 disposition data for:

Cisco Secure Network Analytics / Cisco Stealthwatch  
Management Console / 7.3.0

*Enter additional comments (optional)*



Characters left : 1000

Close

Submit

### **Disposition Data Request Submitted**

The SNA version is currently being evaluated against this vulnerability. This commonly takes less than 10 business days.

---

**Note:** There is no automatic notification that the disposition has been updated. You can save the URL to make revisiting the page easier.

---

## Affected

The SNA version has been evaluated as affected by the bug. A link to the CDETS bug is provided which has more info including potential workarounds and fix versions.

**Affected:** CVE-2022-31676 impacts Cisco Secure Network Analytics / Cisco Stealthwatch Management Console / 7.4.0. [VEX](#)

Cisco Bugs: [CSCw82075](#)

Vulnerability details:

CVSS Base Score: 7.8

Vulnerability Description: VMware Tools (12.0.0, 11.x.y and 10.x.y) contains a local privilege escalation vulnerability. A malicious actor with local non-administrative access to the Guest OS can escalate privileges as a root user in the virtual machine.

---

## Software Support Timelines

Typically a release is covered under Software Maintenance for 12 months post-release and receives Vulnerability and Security Fixes for 18 months post-release. More information about the SNA software

Release Model and release support timeline is available from [Cisco Stealthwatch® Software Release Model and Release Support Timeline Product Bulletin](#).

You can view a table with SNA version support timelines [here](#) .

## **Additional Info**

[Complete CVR Instructions and FAQ including info on Vulnerability Exploitability eXchange \(VEX\)](#)