Evaluate SNA Vulnerabilities with CVR

Contents

Introduction

Looking Up a Vulnerability

Next Steps

- Not Impacted
- Disposition Data is Unavailable
  - Request Assessment
- Disposition Data Request Submitted
- Affected

Software Support Timelines

Additional Info

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'

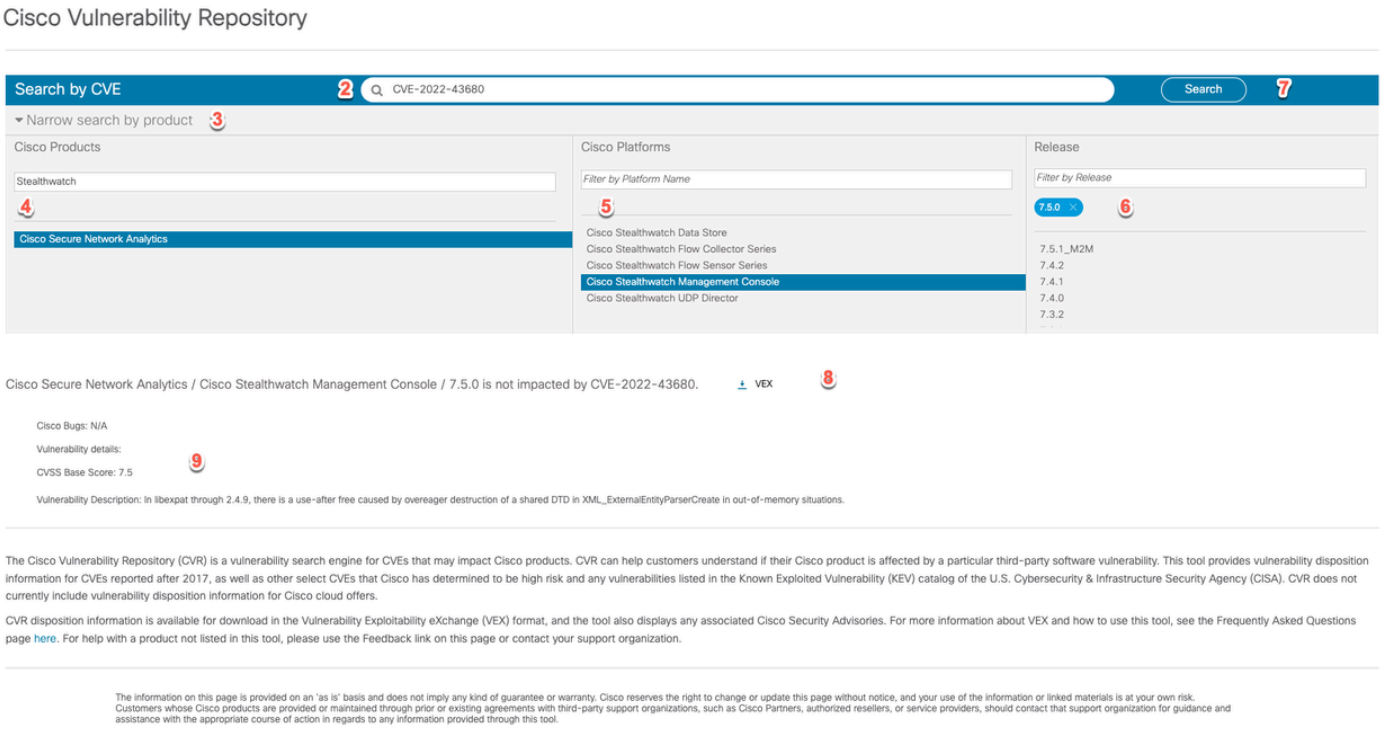
5. In the 'Cisco Platforms' section select the appropriate device type

6. In the 'Release' section select the appropriate version

7. Click 'Search'

8. The disposition reply is displayed after the search is submitted

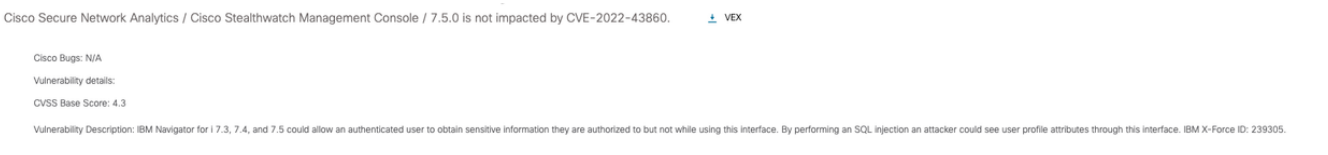
9. You can find additional details to that disposition including links to relevant Cisco Defect and Enhancement Tracking System (CDETS) or the CVSS Base Score



Next Steps

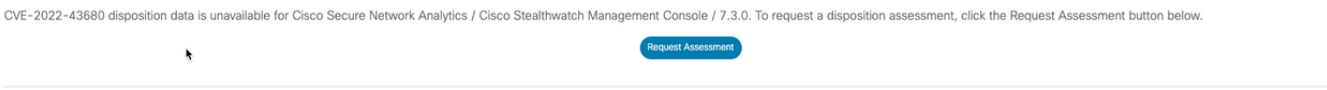
Not Impacted

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



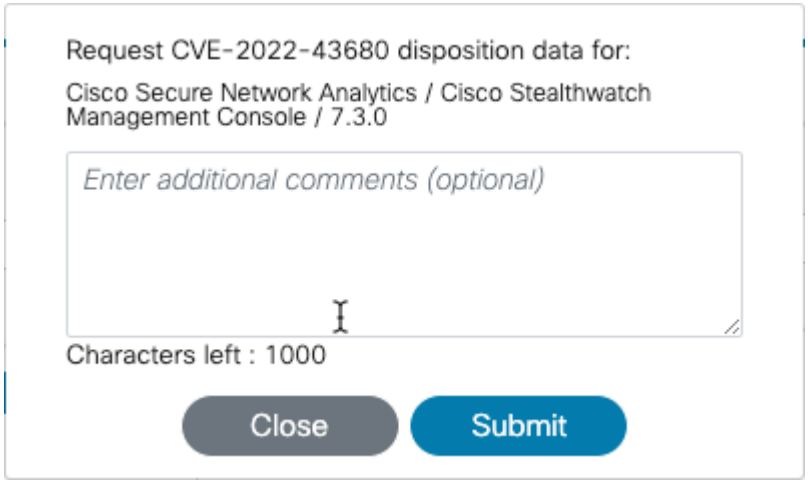
Disposition Data is Unavailable

The SNA version has not be evaluated against this vulnerability.



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".



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.



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)