Identify Network Security Advisories

Security Advisories Overview

The Cisco Product Security Incident Response Team (PSIRT) responds to Cisco product security incidents, regulates the Security Vulnerability Policy, and recommends Cisco Security Advisories and Alerts.

The Security Advisories tool uses these recommended advisories, scans the inventory within Cisco DNA Center, and finds the devices with known vulnerabilities.

View Security Advisories

Before you begin

- To use the Security Advisories tool, you must install the Machine Reasoning package. See *Download and Install Packages and Updates* in the Cisco Digital Network Architecture Center Administrator Guide.
- If you log in to Cisco DNA Center as an Observer, you cannot view the **Security Advisories** tool in the home page.

Step 1 From the Cisco DNA Center home page, scroll down to the **Tools** area, and then click **Security Advisories**. You also can click the icon in the top-right corner and choose **Security Advisories**.

Step 2 If you are launching the **Security Advisories** page for the first time, click **Scan**.

Cisco DNA Center uses the Knowledge Base to identify security issues and improve automated analysis. We recommend that you update the Knowledge Base on a regular basis to view the latest security advisories.

a) Click > **System Settings** > **Settings** > **Machine Reasoning**.
b) Click **Import Latest from Cisco**, or click **here** to download the latest available Knowledge Base, and then click **Import from local**.
c) Click the **AUTO UPDATE** toggle button to subscribe to the automatic update.

Note

- The security advisories dashboard shows security advisories published by Cisco that may affect devices on your network based on the software image currently installed. A further analysis of the configuration, platform details, or other criteria is required to determine if a vulnerability is actually present.
- The security advisories scanning support is only available for routers and switches that comply with the minimum supported software version. For more information on minimum supported software version, see Cisco DNA Center Supported Devices.
- The security advisories displayed are subject to the Cisco Security Vulnerability Policy.

The following table describes the information that is available.

Column	Description
Advisory ID	ID of the security advisories found in the network.
Advisory title	Name of the security vulnerability advisory applicable to the network devices. Click the advisory to go to the respective advisory web page.
CVSS score	Score evaluated based on the Common Vulnerability Scoring System (CVSS) model.
Impact	Impact of the vulnerability on the network, such as Critical, High, Medium, or Low.
CVE	Common Vulnerabilities and Exposures (CVE) identifier for the vulnerability.
Devices	The number of devices impacted by the vulnerability. Click the number to view the devices that may be vulnerable based on this specific advisory, and upgrade the devices as needed.
Known since (days)	The number of days since the vulnerability was discovered.
Last Updated	The date when the advisory was last updated.

Step 3 Click the **Devices** tab to view the number of advisories applicable to each device.

a) Click the number of advisories to view all that match the device.

b) Click the topology icon in the top-right corner to view the device topology. You can click a device in the topology to view all advisories that match the device.

A lock icon next to the device indicates that there are one or more advisories applicable to the device.

Step 4 Click **Scan** at any time to refresh the results displayed.