SECURITY BULLETIN OSB-101719-V1.0

Cisco Aironet Vulnerabilities and Mitigations

CVE-2019-15261, CVE-2019-15264

ORDR SECURITY BULLETIN

Cisco Aironet Vulnerabilities and Mitigations

CVE-2019-15261, CVE-2019-15264

Cisco announced that their popular Aironet Access Points and Catalyst 9100 Access Points are vulnerable to a Denial of Service attack. More information can be found in the below links:

- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191016-airo-capwap-dos
- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191016-airo-pptp-dos
- https://nvd.nist.gov/vuln/detail/CVE-2019-15261
- https://nvd.nist.gov/vuln/detail/CVE-2019-15264

Cisco released software patches and advises customers to upgrade the AP software to the latest compatible version. Below is the table of impacted AP software and the recommended fixed version to use as a patch. Please refer to the Cisco Security Advisory page for the latest update.

CISCO AIRONET AP SOFTWARE MAJOR RELEASE	FIRST FIXED RELEASE FOR THIS VULNERABILITY	RECOMMENDED RELEASE FOR ALL VULNERABILITIES DESCRIBED IN THE COLLECTION OF ADVISORIES
8.2	8.5.151.0	8.5.151.0
8.3	8.5.151.0	8.5.151.0
8.4	8.5.151.0	8.5.151.0
8.5	8.5.151.0	8.5.151.0
8.6	8.8.125.0	8.8.125.0
8.7	8.8.125.0	8.8.125.0
8.8	8.8.125.0	8.8.125.0
8.9	8.9.111.0	8.9.111.0
8.10	Not vulnerable	Not vulnerable

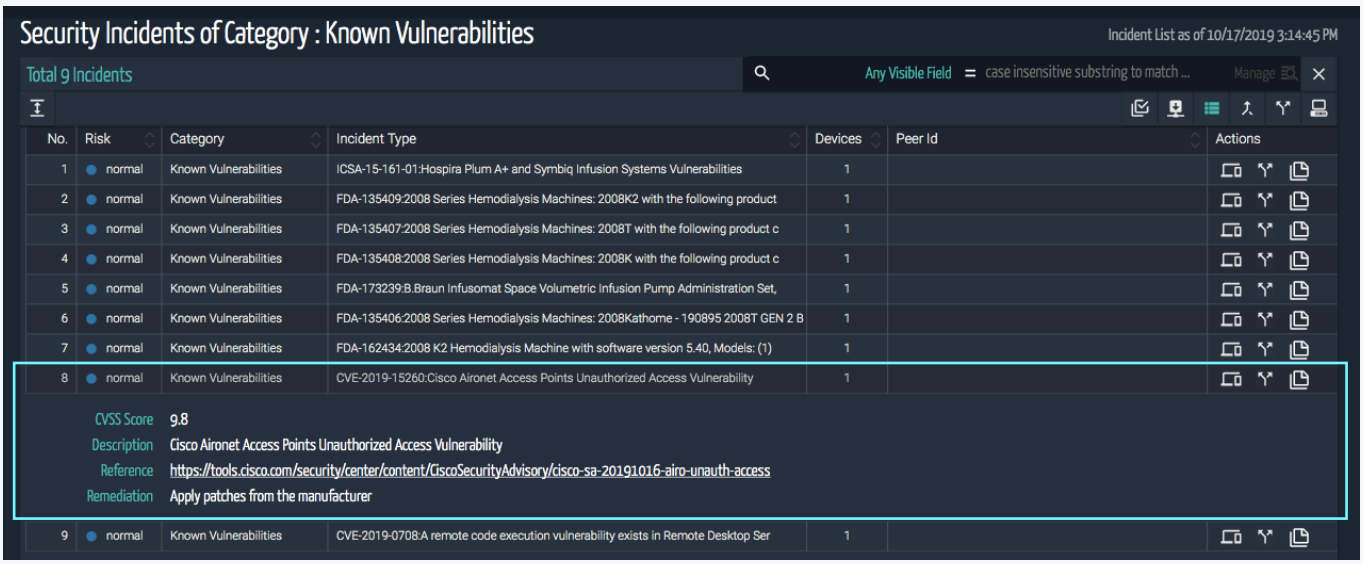
Ordr Systems Control Engine (SCE) has new features that allow customers to quickly identify vulnerable APs and help with the mitigation strategy. Customers subscribed to the Ordr cloud service can determine the affected APs right away. Customers who opted out of Ordr cloud service can work with our customer success team to upgrade the SCE and then assess the situation.

The remainder of this document demonstrates how SCE helps identify vulnerable Cisco APs. It assumes you are using version 7.1(R6) or beyond. If you are using a different version of software and need help navigating to get the information, please contact our local Ordr sales or customer success team.

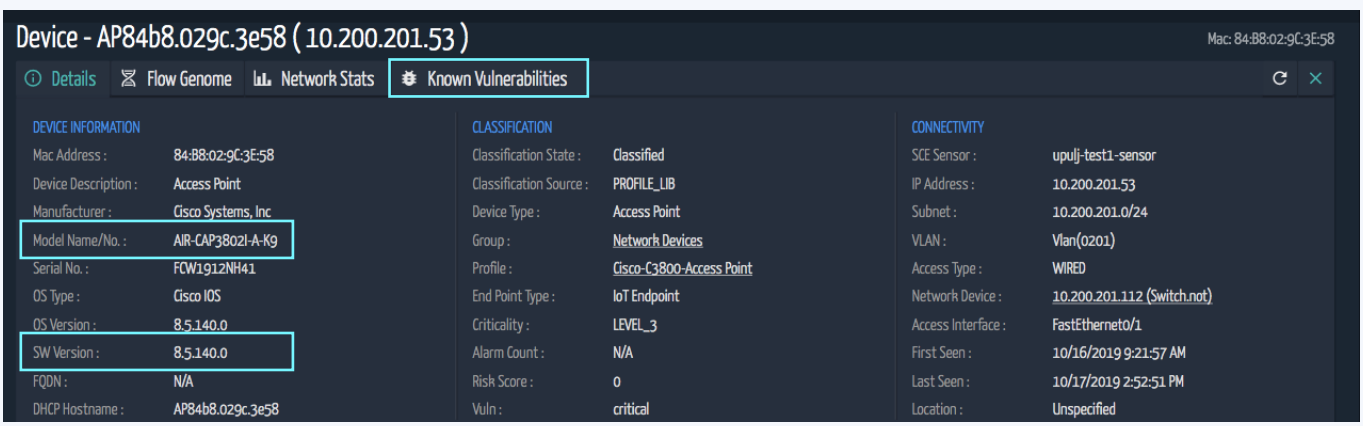
Identify vulnerable APs

The SCE vulnerability database tracks the hardware and software versions of Cisco APs that are vulnerable to CVE-2019-15261 and CVE-2019-15264. You can find a list of them in the **Incident Summary** page under the **Known Vuln** category as shown below.

You will see Cisco Aironet listed as one of the vulnerabilities along with the number of impacted devices. Next, click on the device icon under the Actions column to get a complete listing of the vulnerable Cisco APs. These are the devices you need to patch.

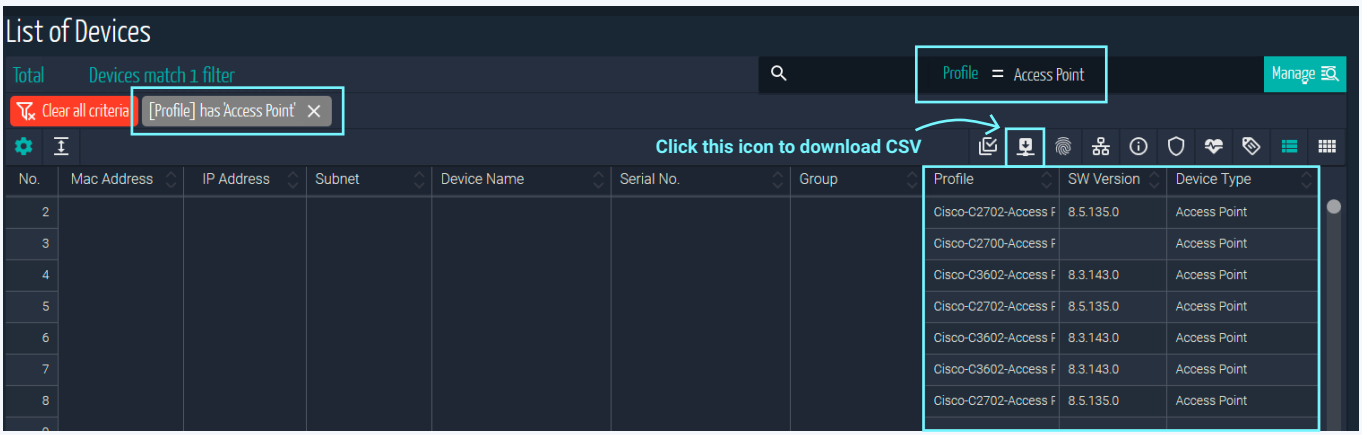


You can also inspect if a specific AP and see what software is installed and determine if it is vulnerable. Go to an AP's Device page. You will see the current software version listed. If the AP is vulnerable, the **Known Vulnerabilities** menu option will display if it needs to be patched, as shown below. Ordr is tracking Cisco's list of affected devices, and the SCE database will update when they are announced.



Identify all AP's in the network

To obtain a list of all the APs in your environment you can go to the Devices menu and filter **"Profile = Access Point"** or **"Device Type = Access Point"**. This will list the APs and their installed software. Please refer to Appendix-1 for more information on how to customize the device view.



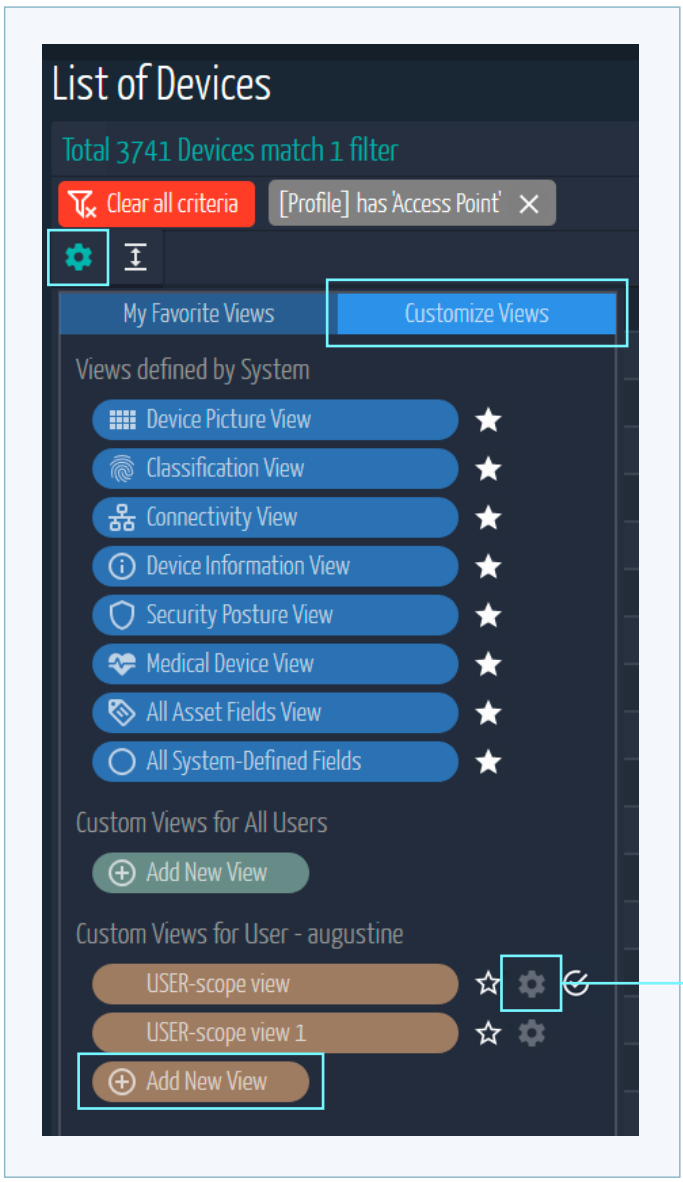
If you want to work offline and generate a spreadsheet of the APs, just click on the **Download CSV** button. This will generate a CSV file.

Note: *Depending on the software release the menu options and buttons might vary a bit. Please contact Ordr Sales or Customer Success team for any assistance.*

Appendix-A:

Customize the devices view by following the below steps:

1. Click on the **Gear** icon in the actions bar, select the **Customize Views** tab, and click on **Add New View**
2. Click on the **Gear** icon next to the newly created USER-scope view
3. Add the columns you would like to see from the **Hidden Columns** section. Click on the **Eye** icon to select the items you want to see. The typical fields to select are IP Address, Subnet, Device Name, Group, Profile, SW Version, Device Type. The important fields that we would be using are Profile and the SW Version.



ōrdr

take control.

info@ordr.net

www.ordr.net

2445 Augustine Drive Suite 601
Santa Clara, CA 95054