



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.

Security Incidents of Category : Known Vulnerabilities

Incident List as of 10/17/2019 3:14:45 PM

Total 9 Incidents

No.	Risk	Category	Incident Type	Devices	Peer Id	Actions
1	normal	Known Vulnerabilities	ICSA-15-161-01:Hospira Plum A+ and Symbiq Infusion Systems Vulnerabilities	1		[Icons]
2	normal	Known Vulnerabilities	FDA-135409:2008 Series Hemodialysis Machines: 2008K2 with the following product	1		[Icons]
3	normal	Known Vulnerabilities	FDA-135407:2008 Series Hemodialysis Machines: 2008T with the following product c	1		[Icons]
4	normal	Known Vulnerabilities	FDA-135408:2008 Series Hemodialysis Machines: 2008K with the following product c	1		[Icons]
5	normal	Known Vulnerabilities	FDA-173239:B.Braun Infusomat Space Volumetric Infusion Pump Administration Set,	1		[Icons]
6	normal	Known Vulnerabilities	FDA-135406:2008 Series Hemodialysis Machines: 2008Kathome - 190895 2008T GEN 2 B	1		[Icons]
7	normal	Known Vulnerabilities	FDA-162434:2008 K2 Hemodialysis Machine with software version 5.40, Models: (1)	1		[Icons]
8	normal	Known Vulnerabilities	CVE-2019-15260: Cisco Aironet Access Points Unauthorized Access Vulnerability	1		[Icons]
<p>CVSS Score 9.8</p> <p>Description Cisco Aironet Access Points Unauthorized Access Vulnerability</p> <p>Reference https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191016-airo-unauth-access</p> <p>Remediation Apply patches from the manufacturer</p>						
9	normal	Known Vulnerabilities	CVE-2019-0708: A remote code execution vulnerability exists in Remote Desktop Ser	1		[Icons]

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.

Device - AP84b8.029c.3e58 (10.200.201.53)

Mac: 84-B8-02-9C-3E-58

Details | Flow Genome | Network Stats | **Known Vulnerabilities**

DEVICE INFORMATION	CLASSIFICATION	CONNECTIVITY
Mac Address : 84-B8-02-9C-3E-58	Classification State : Classified	SCE Sensor : upulj-test1-sensor
Device Description : Access Point	Classification Source : PROFILE_LUB	IP Address : 10.200.201.53
Manufacturer : Cisco Systems, Inc	Device Type : Access Point	Subnet : 10.200.201.0/24
Model Name/No. : AIR-CAP3802I-A-K9	Group : Network Devices	VLAN : Vlan(0201)
Serial No. : FQW1912NH41	Profile : Cisco-C3800-Access Point	Access Type : WIRED
OS Type : Cisco IOS	End Point Type : IoT Endpoint	Network Device : 10.200.201.112 (Switch not)
OS Version : 8.5.140.0	Criticality : LEVEL_3	Access Interface : FastEthernet0/1
SW Version : 8.5.140.0	Alarm Count : N/A	First Seen : 10/16/2019 9:21:57 AM
FQDN : N/A	Risk Score : 0	Last Seen : 10/17/2019 2:52:51 PM
DHCP Hostname : AP84b8.029c.3e58	Vuln : critical	Location : Unspecified

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.

The screenshot shows the 'List of Devices' interface with the following data:

No.	Mac Address	IP Address	Subnet	Device Name	Serial No.	Group	Profile	SW Version	Device Type
2							Cisco-C2702-Access F	8.5.135.0	Access Point
3							Cisco-C2700-Access F		Access Point
4							Cisco-C3602-Access F	8.3.143.0	Access Point
5							Cisco-C2702-Access F	8.5.135.0	Access Point
6							Cisco-C3602-Access F	8.3.143.0	Access Point
7							Cisco-C3602-Access F	8.3.143.0	Access Point
8							Cisco-C2702-Access F	8.5.135.0	Access Point

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.

The image consists of two side-by-side screenshots from the Cisco Aironet management interface, illustrating the steps to customize a device view.

Left Screenshot: Shows the 'List of Devices' page. At the top, it indicates 'Total 3741 Devices match 1 filter' with a filter '[Profile] has 'Access Point''. Below this is a 'Clear all criteria' button and a filter input field. A gear icon and a list icon are visible in the top left. The 'Customize Views' tab is highlighted in blue. Under 'Views defined by System', several predefined views are listed with star icons. Under 'Custom Views for All Users', there is an 'Add New View' button. Under 'Custom Views for User - augustine', there are two views: 'USER-scope view' and 'USER-scope view 1', both with star and gear icons. A gear icon next to 'USER-scope view' is highlighted with a red box, and a red arrow points from it to the right screenshot.

Right Screenshot: Shows the 'Hidden Columns' configuration screen. It lists various fields with checkboxes and eye icons to toggle visibility. The fields listed are: Profile, SW Version, Device Type, Access Interface, Access Type, Access Type & Interface, Active Duty Schedule, AD Org Unit, Alarm Count, AntiVirus SW, Auth Method, BL status, Cert Expiry, Cert Issuer Name, Cert Subject, and Cert Validity After. The 'Cert Subject' field has its eye icon checked and is highlighted with a red box. At the bottom, there are 'Cancel', 'Save Change', and 'Delete View' buttons.

ōrdr

take control.



info@ordr.net



www.ordr.net



2445 Augustine Drive Suite 601
Santa Clara, CA 95054