Aggregation and Fragmentation Attacks

Q **What is this security advisory about?**

A Security researchers have identified vulnerabilities in the standards and implementation of some Wi-Fi devices. The Wi-Fi Alliance has taken immediate steps to ensure that users can remain confident in the strong security protections provided by Wi-Fi. The alliance's statement can be found at https://www.wi-fi.org/security-update-fragmentation.

This advisory is based on identified vulnerabilities in the frame aggregation functionality in some Wi-Fi devices and in the frame fragmentation functionality in other devices. These vulnerabilities could allow an attacker to forge encrypted frames, which could in turn enable the exfiltration of sensitive data from a targeted device.

The Wi-Fi Alliance says, "There is no evidence of the vulnerabilities being used against Wi-Fi users maliciously and these issues are mitigated through routine device updates that enable detection of suspect transmissions or improve adherence to recommended security implementation practices."

The Wi-Fi Alliance and the Industry Consortium for Advancement of Security on the Internet (ICASI) coordinated the public response to this attack after evaluating the risks for current Wi-Fi implementations. https://www.icasi.org/aggregation-fragmentation-attacks-against-wifi/.

Q **What is Cisco's guidance on the impact of this security advisory? What steps has Cisco taken to address this?**

A Cisco has been actively engaged with the Wi-Fi Alliance and ICASI since the issues were detected. In order for these attacks to be successful, they require an uncommon configuration and active user participation. Some of the identified vulnerabilities have been theoretically possible for many years, but there is **no evidence of these theoretical vulnerabilities having been or currently being used against Wi-Fi users maliciously**.

These issues are of medium impact and are mitigated through routine device updates that enable detection of suspect transmissions or improve adherence to recommended security implementation practices. Cisco is already in the process of addressing these issues with patches in upcoming software releases.

For more details, see below.

Q

What is the vulnerability, the products affected, and the expected timeline to resolve this issue?

A

Cisco will continue to update this security advisory with information about affected products. Most of the vulnerabilities affect wireless clients. Three vulnerabilities affect access points. All vulnerabilities identified are medium impact only. After the advisory is marked Final, customers should refer to the associated Cisco bug(s) for further details.

Although the risk of an attack is low, since it requires a man-in-the-middle position and victim participation, Cisco recommends upgrading to latest software with the fix.

The table below summarizes the products impacted and fix releases.

Table 1. Products affected and fix releases

Wireless standard	Vulnerable APs	Fix release	Wireless controller support
802.11ax	Catalyst® 9120AX, 9115AX, 9105AX Series	8.10MR6, 16.12.6, 17.3.4, 17.6.1	Catalyst 9800 Series, Cisco® 3504, 5520, 8540, Virtual Wireless Controller (vWLC), Mobility Express (ME)
	Catalyst 9130AX, 9117AX, 9124AX Series	8.10MR6, 17.3.4, 17.6.1 (9124AX only in 17.6.1 and not in AireOS)	Catalyst 9800 Series, Cisco 3504, 5520, 8540, vWLC, ME
802.11ac Wave 2	Aironet® 1562, 2802, 3802, 4800 Series	8.5MR8, 8.10MR6, 17.3.4, 16.12.6, 17.6.1	Catalyst 9800 Series, Cisco 3504, 5520, 8540, 2504, 5508, 8510, vWLC , ME
	Aironet 1542, 1810, 1815, 1832, 1840, 1852, 1800i	8.5MR8, 8.10MR6, 17.3.4, 16.12.6, 17.6.1	
802.11ac Wave 1	Aironet 1572, 1702, 2702, 3702	8.5MR8, 8.10MR6, 17.3.4, 16.12.6	Catalyst 9800 Series, Cisco 3504, 5520, 8540, 2504, 5508, 8510, vWLC, Wireless Services Module 2 (WiSM2), ME
802.11n	Aironet 1552	8.5MR8, 8.10MR6	Cisco 3504, 5520, 8540, 2504, 5508, 8510, vWLC, WiSM2, ME
	Aironet 1532	Impact under evaluation*	-

*Some of the bug fixes are dependent on chipset vendors providing the fix. Cisco is working with the chipset vendors to ensure a robust and quality fix for all our access points.

Table 2. Timeline for fix releases

Release	Timeline
8.10MR6/17.3.4	June 2021
17.6.1	July 2021
16.12.6	August 2021
8.5MR8	August 2021

Q **Will fixes be available for end-of-life APs as well?**

A All end-of-sale access points in the table above that are still under End of Vulnerability support will be provided with fixes in upcoming software releases. These include the Catalyst 9117AX Series, Aironet 1800i, and 802.11ac Wave 1 and 802.11n devices.

Q **Why can't these fixes be made available immediately?**

A Cisco is the industry leader with a wide variety and maximum installed base of access points across 802.11n, 802.11ac Wave 1 and Wave 2, and Wi-Fi 6, with multiple releases and different source code bases. Cisco is performing thorough testing across the source code with both clients and access points requiring a patch. Cisco is also working with all affected access point chipset vendors to ensure that driver fixes are complete and integrated into Cisco's software release fixes across all APs and chipsets with our timelines.

Q **What are some key best practices Cisco is using to mitigate this attack?**

A Our containment for a Valid Client that connects to this rogue with rogue detection could mitigate this attack.

Q **Who can I reach out to for specific customer incidents?**

A This impacts select configurations only. If escalation images are needed please work with account team or channel teams. Requests will be evaluated based on business and security justification.

For more information on Cisco wireless, visit: https://www.cisco.com/c/en/us/products/wireless/index.html.

C67-744966-00 06/21