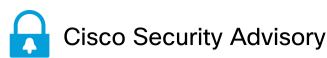




Log in



[Home](#) / [Cisco Security](#) / [Security Advisories](#)



# Multiple Vulnerabilities in Frame Aggregation and Fragmentation Implementations of 802.11 Specification Affecting Cisco Products: May 2021

**Advisory ID:**

cisco-sa-wifi-faf-22epcEWu

**First Published:**

2021 May 11 18:00 GMT

**Last Updated:**

2021 December 15 15:47 GMT

**Version 1.9:** [Final](#)**Workarounds:** No workarounds available**Cisco Bug IDs:**[CSCvx24420](#) , [CSCvx24423](#) , [CSCvx24425](#) , [More...](#)

CVE-2020-24586

CVE-2020-24587

CVE-2020-24588

[More...](#)

CWE-345

CWE-772

CWE-99

**CVSS Score:**[Base 6.5](#) [Download CSAF](#)[Email](#)

## Summary

On May 11, 2021, the research paper *Fragment and Forge: Breaking Wi-Fi Through Frame Aggregation and Fragmentation* was made public. This paper discusses 12 vulnerabilities in the 802.11 standard. One vulnerability is in the frame aggregation functionality, two vulnerabilities are in the frame fragmentation functionality, and the other nine are implementation vulnerabilities. These vulnerabilities could allow an attacker to forge encrypted frames, which could in turn enable the exfiltration of sensitive data from a targeted device.

This advisory will be updated as additional information becomes available.

This advisory is available at the following link:

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wifi-faf-22epcEWu>

## Affected Products

Cisco is investigating its product line to determine which products may be affected by these vulnerabilities. As the investigation progresses, Cisco will update this advisory with information about affected products.

### Vulnerable Products

The following table lists Cisco products that are affected by the vulnerabilities that are described in this advisory. If a future release date is indicated for software, the date provided represents an estimate based on all information known to Cisco as of the Last Updated date at the top of the advisory. Availability dates are subject to change based on a number of factors, including satisfactory testing results and delivery of other priority features and fixes. If no version or date is listed for an affected component (indicated by a blank field and/or an advisory designation of Interim), Cisco is continuing to evaluate the fix and will update the advisory as additional information becomes available. After the advisory is marked Final, customers should refer to the associated Cisco bug(s) for further details.

| CVE ID  | Cisco Bug ID               | Fixed Release Availability                       |
|---|----------------------------|--|
| Aironet 1532 APs, AP803 Integrated AP on IR829 Industrial Integrated Services Routers   |                            |  |
| CVE-2020-24586  | <a href="#">CSCvy32690</a> | 8.5MR8<br>8.10MR6                                |
| CVE-2020-24587  | <a href="#">CSCvy32690</a> | 8.5MR8<br>8.10MR6                                |
| CVE-2020-24588  | <a href="#">CSCvy32690</a> | 8.5MR8<br>8.10MR6                                |
| CVE-2020-26139  | Not affected               | N/A  |
| CVE-2020-26140  | Not affected               | N/A  |
| CVE-2020-26141  | Not affected               | N/A  |
| CVE-2020-26142  | Not affected               | N/A  |
| CVE-2020-26143  | Not affected               | N/A  |
| CVE-2020-26144  | Not affected               | N/A  |
| CVE-2020-26145  | Not affected               | N/A  |
| CVE-2020-26146  | Not affected               | N/A  |
| CVE-2020-26147  | Not affected               | N/A  |
| Aironet 1542 APs, Aironet 1810 APs, Aironet 1815 APs, Aironet 1832 APs, Aironet 1842 APs, Aironet 1852 APs, Aironet 1800i APs   |                            |  |
| CVE-2020-24586  | Not affected               | N/A  |
| CVE-2020-24587  | <a href="#">CSCvx24420</a> | 8.5MR8<br>8.10MR6<br>16.12.6<br>17.3.4<br>17.6.1 |
| CVE-2020-24588  | <a href="#">CSCvx24420</a> | 8.5MR8<br>8.10MR6<br>16.12.6<br>17.3.4<br>17.6.1 |
| CVE-2020-26139  | <a href="#">CSCvx24420</a> | 8.5MR8<br>8.10MR6<br>16.12.6<br>17.3.4<br>17.6.1 |
| CVE-2020-26140  | Not affected               | N/A  |
| CVE-2020-26141  | Not affected               | N/A  |
| CVE-2020-26142  | Not affected               | N/A  |
| CVE-2020-26143  | Not affected               | N/A  |
| CVE-2020-26144  | Not affected               | N/A  |
| CVE-2020-26145  | <a href="#">CSCvx24420</a> | 8.5MR8<br>8.10MR6<br>16.12.6<br>17.3.4<br>17.6.1 |
| CVE-2020-26146  | <a href="#">CSCvx24420</a> | 8.5MR8<br>8.10MR6<br>16.12.6<br>17.3.4<br>17.6.1 |
| CVE-2020-26147  | Not affected               | N/A  |
| Aironet 1552 APs, Aironet 1552H APs, Aironet 1572 APs, Aironet 1702 APs, Aironet 2702 APs, Aironet 3702 APs, IW 3702 APs  |                            |  |
| CVE-2020-24586  | <a href="#">CSCvy32680</a> | 8.5MR8<br>8.10MR6<br>16.12.6<br>17.3.4           |
| CVE-2020-24587  | <a href="#">CSCvy32680</a> | 8.5MR8<br>8.10MR6<br>16.12.6<br>17.3.4           |
| CVE-2020-24588  | Not affected               | N/A  |
| CVE-2020-26139  | Not affected               | N/A  |
| CVE-2020-26140  | Not affected               | N/A  |
| CVE-2020-26141  | Not affected               | N/A  |
| CVE-2020-26142  | Not affected               | N/A  |
| CVE-2020-26143  | Not affected               | N/A  |
| CVE-2020-26144  | Not affected               | N/A  |
| CVE-2020-26145  | Not affected               | N/A  |
| CVE-2020-26146  | Not affected               | N/A  |
| CVE-2020-26147  | Not affected               | N/A  |
| Aironet 1560 Series APs, Aironet 2800 Series APs, Aironet Series 3800 APs, Aironet Series 4800 APs, Catalyst IW 6300 APs, 6300 Series Embedded Services APs (ESW6300) |                            |  |
| CVE-2020-24586  | <a href="#">CSCvx24449</a> | 8.5MR8<br>8.10MR6<br>16.12.6<br>17.3.4<br>17.6.1 |

|  |                            |  |
|--|----------------------------|--|
| CVE-2020-24587   | <a href="#">CSCvx24449</a> | 8.5MR8<br>8.10MR6<br>16.12.6<br>17.3.4<br>17.6.1 |
| CVE-2020-24588   | Not affected               | N/A  |
| CVE-2020-26139   | Not affected               | N/A  |
| CVE-2020-26140   | <a href="#">CSCvy36698</a> | 8.5MR8<br>8.10MR6<br>16.12.6<br>17.3.4<br>17.6.1 |
| CVE-2020-26141   | Not affected               | N/A  |
| CVE-2020-26142   | Not affected               | N/A  |
| CVE-2020-26143   | <a href="#">CSCvy36698</a> | 8.5MR8<br>8.10MR6<br>16.12.6<br>17.3.4<br>17.6.1 |
| CVE-2020-26144   | Not affected               | N/A  |
| CVE-2020-26145   | Not affected               | N/A  |
| CVE-2020-26146   | <a href="#">CSCvy36698</a> | 8.5MR8<br>8.10MR6<br>16.12.6<br>17.3.4<br>17.6.1 |
| CVE-2020-26147   | <a href="#">CSCvy36698</a> | 8.5MR8<br>8.10MR6<br>16.12.6<br>17.3.4<br>17.6.1 |
| Catalyst 9105 APs, Catalyst 9115 APs, Catalyst 9120 APs, Integrated AP on 1100 Integrated Services Routers |                            |  |
| CVE-2020-24586   | <a href="#">CSCvx24425</a> | 8.10MR6<br>16.12.6<br>17.3.4<br>17.6.1           |
| CVE-2020-24587   | <a href="#">CSCvx24425</a> | 8.10MR6<br>16.12.6<br>17.3.4<br>17.6.1           |
| CVE-2020-24588   | <a href="#">CSCvx24425</a> | 8.10MR6<br>16.12.6<br>17.3.4<br>17.6.1           |
| CVE-2020-26139   | Not affected               | N/A  |
| CVE-2020-26140   | Not affected               | N/A  |
| CVE-2020-26141   | Not affected               | N/A  |
| CVE-2020-26142   | Not affected               | N/A  |
| CVE-2020-26143   | Not affected               | N/A  |
| CVE-2020-26144   | Not affected               | N/A  |
| CVE-2020-26145   | Not affected               | N/A  |
| CVE-2020-26146   | Not affected               | N/A  |
| CVE-2020-26147   | Not affected               | N/A  |
| Catalyst 9117 APs  |                            |  |
| CVE-2020-24586   | <a href="#">CSCvx24439</a> | 8.10MR6<br>16.12.6<br>17.3.4<br>17.6.1           |
| CVE-2020-24587   | <a href="#">CSCvx24439</a> | 8.10MR6<br>16.12.6<br>17.3.4<br>17.6.1           |
| CVE-2020-24588   | <a href="#">CSCvx24439</a> | 8.10MR6<br>16.12.6<br>17.3.4<br>17.6.1           |
| CVE-2020-26139   | <a href="#">CSCvx24439</a> | 8.10MR6<br>16.12.6<br>17.3.4<br>17.6.1           |
| CVE-2020-26140   | Not affected               | N/A  |
| CVE-2020-26141   | Not affected               | N/A  |
| CVE-2020-26142   | Not affected               | N/A  |
| CVE-2020-26143   | Not affected               | N/A  |
| CVE-2020-26144   | <a href="#">CSCvx24439</a> | 8.10MR6<br>16.12.6<br>17.3.4<br>17.6.1           |

|   |  |  |
|---|--|--|
| CVE-2020-26145  | <a href="#">CSCvx24439</a>   | 8.10MR6<br>16.12.6<br>17.3.4<br>17.6.1 |
| CVE-2020-26146  | <a href="#">CSCvx24439</a>   | 8.10MR6<br>16.12.6<br>17.3.4<br>17.6.1 |
| CVE-2020-26147  | Not affected   | N/A                                    |
| Catalyst 9124 APs <sup>1</sup> , Catalyst 9130 APs  |  |  |
| CVE-2020-24586  | <a href="#">CSCvx24428</a><br><a href="#">CSCvx24452</a><br><a href="#">CSCvx24456</a> | 8.10MR6<br>16.12.6<br>17.3.4<br>17.6.1 |
| CVE-2020-24587  | <a href="#">CSCvx24428</a><br><a href="#">CSCvx24452</a><br><a href="#">CSCvx24456</a> | 8.10MR6<br>16.12.6<br>17.3.4<br>17.6.1 |
| CVE-2020-24588  | <a href="#">CSCvx24428</a><br><a href="#">CSCvx24452</a><br><a href="#">CSCvx24456</a> | 8.10MR6<br>16.12.6<br>17.3.4<br>17.6.1 |
| CVE-2020-26139  | <a href="#">CSCvx24428</a><br><a href="#">CSCvx24452</a><br><a href="#">CSCvx24456</a> | 8.10MR6<br>16.12.6<br>17.3.4<br>17.6.1 |
| CVE-2020-26140  | Not affected   | N/A                                    |
| CVE-2020-26141  | Not affected   | N/A                                    |
| CVE-2020-26142  | Not affected   | N/A                                    |
| CVE-2020-26143  | Not affected   | N/A                                    |
| CVE-2020-26144  | <a href="#">CSCvx24428</a><br><a href="#">CSCvx24452</a><br><a href="#">CSCvx24456</a> | 8.10MR6<br>16.12.6<br>17.3.4<br>17.6.1 |
| CVE-2020-26145  | <a href="#">CSCvx24428</a><br><a href="#">CSCvx24452</a><br><a href="#">CSCvx24456</a> | 8.10MR6<br>16.12.6<br>17.3.4<br>17.6.1 |
| CVE-2020-26146  | <a href="#">CSCvx24428</a><br><a href="#">CSCvx24452</a><br><a href="#">CSCvx24456</a> | 8.10MR6<br>16.12.6<br>17.3.4<br>17.6.1 |
| CVE-2020-26147  | Not affected   | N/A                                    |
| 1. Catalyst 9124 APs were not supported until Release 17.5, and the fix will be available in Release 17.6.1                                   |  |  |
| Meraki GR10, GR60, MR20, MR30H, MR33, MR36, MR42, MR42E, MR44, MR45, MR46, MR46E, MR52, MR53, MR53E, MR55, MR56, MR70, MR74, MR76, MR84, MR86 |  |  |
| CVE-2020-24586  | No bug ID  | MR 27.7.1                              |
| CVE-2020-24587  | No bug ID  | MR 27.7.1                              |
| CVE-2020-24588  | No bug ID  | MR 27.7.1                              |
| CVE-2020-26139  | No bug ID  | MR 27.7.1                              |
| CVE-2020-26140  | No bug ID  | MR 27.7.1                              |
| CVE-2020-26141  | No bug ID  | MR 27.7.1                              |
| CVE-2020-26142  | No bug ID  | MR 27.7.1                              |
| CVE-2020-26143  | No bug ID  | MR 27.7.1                              |
| CVE-2020-26144  | No bug ID  | MR 27.7.1                              |
| CVE-2020-26145  | No bug ID  | MR 27.7.1                              |
| CVE-2020-26146  | No bug ID  | MR 27.7.1                              |
| CVE-2020-26147  | No bug ID  | MR 27.7.1                              |
| Meraki MR12, MR18, MR26, MR32, MR34, MR62, MR66, MR72   |  |  |
| CVE-2020-24586  | No bug ID  | MR 26.8.3                              |
| CVE-2020-24587  | No bug ID  | MR 26.8.3                              |
| CVE-2020-24588  | No bug ID  | MR 26.8.3                              |
| CVE-2020-26139  | No bug ID  | MR 26.8.3                              |
| CVE-2020-26140  | No bug ID  | MR 26.8.3                              |
| CVE-2020-26141  | No bug ID  | MR 26.8.3                              |
| CVE-2020-26142  | No bug ID  | MR 26.8.3                              |
| CVE-2020-26143  | No bug ID  | MR 26.8.3                              |
| CVE-2020-26144  | No bug ID  | MR 26.8.3                              |
| CVE-2020-26145  | No bug ID  | MR 26.8.3                              |
| CVE-2020-26146  | No bug ID  | MR 26.8.3                              |
| CVE-2020-26147  | No bug ID  | MR 26.8.3                              |
| Meraki MX64W, MX65W, MX67W, MX67CW, MX68W, MX68CW, Z3, Z3C <sup>1</sup>   |  |  |
| CVE-2020-24586  | No bug ID  | MX 17.0                                |
| CVE-2020-24587  | No bug ID  | MX 17.0                                |
| CVE-2020-24588  | No bug ID  | MX 17.0                                |

|  |                            |            |
|--|----------------------------|------------|
| CVE-2020-26139   | No bug ID                  | MX 17.0    |
| CVE-2020-26140   | No bug ID                  | MX 17.0    |
| CVE-2020-26141   | No bug ID                  | MX 17.0    |
| CVE-2020-26142   | No bug ID                  | MX 17.0    |
| CVE-2020-26143   | No bug ID                  | MX 17.0    |
| CVE-2020-26144   | No bug ID                  | MX 17.0    |
| CVE-2020-26145   | No bug ID                  | MX 17.0    |
| CVE-2020-26146   | No bug ID                  | MX 17.0    |
| CVE-2020-26147   | No bug ID                  | MX 17.0    |
| 1. Cisco will not fix these vulnerabilities in the following Cisco Meraki products: MX60W and Z1 |                            |            |
| IP Phone 8861, IP Phone 8865, and IP Conference Phone 8832                                       |                            |            |
| CVE-2020-24586   | <a href="#">CSCvx60997</a> | 14.1(1)    |
| CVE-2020-24587   | <a href="#">CSCvx60997</a> | 14.1(1)    |
| CVE-2020-24588   | <a href="#">CSCvx60997</a> | 14.1(1)    |
| CVE-2020-26139   | <a href="#">CSCvx60997</a> | 14.1(1)    |
| CVE-2020-26140   | <a href="#">CSCvx60997</a> | 14.1(1)    |
| CVE-2020-26141   | <a href="#">CSCvx60997</a> | 14.1(1)    |
| CVE-2020-26142   | <a href="#">CSCvx60997</a> | 14.1(1)    |
| CVE-2020-26143   | <a href="#">CSCvx60997</a> | 14.1(1)    |
| CVE-2020-26144   | <a href="#">CSCvx60997</a> | 14.1(1)    |
| CVE-2020-26145   | <a href="#">CSCvx60997</a> | 14.1(1)    |
| CVE-2020-26146   | <a href="#">CSCvx60997</a> | 14.1(1)    |
| CVE-2020-26147   | <a href="#">CSCvx60997</a> | 14.1(1)    |
| IP Phone 6861 and IP Phone 8861 Running Third-Party Call Control (3PCC) Software                 |                            |            |
| CVE-2020-24586   | <a href="#">CSCvx61001</a> | 11.3(5)    |
| CVE-2020-24587   | <a href="#">CSCvx61001</a> | 11.3(5)    |
| CVE-2020-24588   | <a href="#">CSCvx61001</a> | 11.3(5)    |
| CVE-2020-26139   | <a href="#">CSCvx61001</a> | 11.3(5)    |
| CVE-2020-26140   | <a href="#">CSCvx61001</a> | 11.3(5)    |
| CVE-2020-26141   | <a href="#">CSCvx61001</a> | 11.3(5)    |
| CVE-2020-26142   | <a href="#">CSCvx61001</a> | 11.3(5)    |
| CVE-2020-26143   | <a href="#">CSCvx61001</a> | 11.3(5)    |
| CVE-2020-26144   | <a href="#">CSCvx61001</a> | 11.3(5)    |
| CVE-2020-26145   | <a href="#">CSCvx61001</a> | 11.3(5)    |
| CVE-2020-26146   | <a href="#">CSCvx61001</a> | 11.3(5)    |
| CVE-2020-26147   | <a href="#">CSCvx61001</a> | 11.3(5)    |
| Wireless IP Phone 8821   |                            |            |
| CVE-2020-24586   | <a href="#">CSCvx61012</a> | 11.0(6)SR2 |
| CVE-2020-24587   | <a href="#">CSCvx61012</a> | 11.0(6)SR2 |
| CVE-2020-24588   | <a href="#">CSCvx61012</a> | 11.0(6)SR2 |
| CVE-2020-26139   | <a href="#">CSCvx61012</a> | 11.0(6)SR2 |
| CVE-2020-26140   | <a href="#">CSCvx61012</a> | 11.0(6)SR2 |
| CVE-2020-26141   | <a href="#">CSCvx61012</a> | 11.0(6)SR2 |
| CVE-2020-26142   | <a href="#">CSCvx61012</a> | 11.0(6)SR2 |
| CVE-2020-26143   | <a href="#">CSCvx61012</a> | 11.0(6)SR2 |
| CVE-2020-26144   | <a href="#">CSCvx61012</a> | 11.0(6)SR2 |
| CVE-2020-26145   | <a href="#">CSCvx61012</a> | 11.0(6)SR2 |
| CVE-2020-26146   | <a href="#">CSCvx61012</a> | 11.0(6)SR2 |
| CVE-2020-26147   | <a href="#">CSCvx61012</a> | 11.0(6)SR2 |
| Webex Desk Series and Webex Room Series  |                            |            |
| CVE-2020-24586   | <a href="#">CSCvx89821</a> | 1.2(0)SR1  |
| CVE-2020-24587   | <a href="#">CSCvx89821</a> | 1.2(0)SR1  |
| CVE-2020-24588   | <a href="#">CSCvx89821</a> | 1.2(0)SR1  |
| CVE-2020-26139   | <a href="#">CSCvx89821</a> | 1.2(0)SR1  |
| CVE-2020-26140   | <a href="#">CSCvx89821</a> | 1.2(0)SR1  |
| CVE-2020-26141   | <a href="#">CSCvx89821</a> | 1.2(0)SR1  |
| CVE-2020-26142   | <a href="#">CSCvx89821</a> | 1.2(0)SR1  |
| CVE-2020-26143   | <a href="#">CSCvx89821</a> | 1.2(0)SR1  |
| CVE-2020-26144   | <a href="#">CSCvx89821</a> | 1.2(0)SR1  |
| CVE-2020-26145   | <a href="#">CSCvx89821</a> | 1.2(0)SR1  |
| CVE-2020-26146   | <a href="#">CSCvx89821</a> | 1.2(0)SR1  |
| CVE-2020-26147   | <a href="#">CSCvx89821</a> | 1.2(0)SR1  |
| Webex Board Series   |                            |            |
| CVE-2020-24586   | <a href="#">CSCvx61020</a> | 10.8.2.5   |
| CVE-2020-24587   | <a href="#">CSCvx61020</a> | 10.8.2.5   |
| CVE-2020-24588   | <a href="#">CSCvx61020</a> | 10.8.2.5   |

|                                  |                            |          |
|----------------------------------|----------------------------|----------|
| CVE-2020-26139                   | <a href="#">CSCvx61020</a> | 10.8.2.5 |
| CVE-2020-26140                   | <a href="#">CSCvx61020</a> | 10.8.2.5 |
| CVE-2020-26141                   | <a href="#">CSCvx61020</a> | 10.8.2.5 |
| CVE-2020-26142                   | <a href="#">CSCvx61020</a> | 10.8.2.5 |
| CVE-2020-26143                   | <a href="#">CSCvx61020</a> | 10.8.2.5 |
| CVE-2020-26144                   | <a href="#">CSCvx61020</a> | 10.8.2.5 |
| CVE-2020-26145                   | <a href="#">CSCvx61020</a> | 10.8.2.5 |
| CVE-2020-26146                   | <a href="#">CSCvx61020</a> | 10.8.2.5 |
| CVE-2020-26147                   | <a href="#">CSCvx61020</a> | 10.8.2.5 |
| Webex Wireless Phone 840 and 860 |                            |          |
| CVE-2020-24586                   | <a href="#">CSCvx62886</a> | 1.4(0)   |
| CVE-2020-24587                   | <a href="#">CSCvx62886</a> | 1.4(0)   |
| CVE-2020-24588                   | <a href="#">CSCvx62886</a> | 1.4(0)   |
| CVE-2020-26139                   | <a href="#">CSCvx62886</a> | 1.4(0)   |
| CVE-2020-26140                   | <a href="#">CSCvx62886</a> | 1.4(0)   |
| CVE-2020-26141                   | <a href="#">CSCvx62886</a> | 1.4(0)   |
| CVE-2020-26142                   | <a href="#">CSCvx62886</a> | 1.4(0)   |
| CVE-2020-26143                   | <a href="#">CSCvx62886</a> | 1.4(0)   |
| CVE-2020-26144                   | <a href="#">CSCvx62886</a> | 1.4(0)   |
| CVE-2020-26145                   | <a href="#">CSCvx62886</a> | 1.4(0)   |
| CVE-2020-26146                   | <a href="#">CSCvx62886</a> | 1.4(0)   |
| CVE-2020-26147                   | <a href="#">CSCvx62886</a> | 1.4(0)   |

## Products Confirmed Not Vulnerable

Only products listed in the [Vulnerable Products](#) section of this advisory are known to be affected by this vulnerability.

## ^ Details

The vulnerabilities are not dependent on one another. Exploitation of one of the vulnerabilities is not required to exploit another vulnerability. In addition, a software release that is affected by one of the vulnerabilities may not be affected by the other vulnerabilities.

For a description of the following vulnerabilities, see [Fragment and Forge: Breaking Wi-Fi Through Frame Aggregation and Fragmentation](#).

For additional information, see [FragAttacks](#).

### CVE-2020-26140: Accepting plaintext data frames in a protected network

Security Impact Rating (SIR): Medium

CVSS Base Score: 6.5

CVSS Vector: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

### CVE-2020-26143: Accepting fragmented plaintext data frames in a protected network

Security Impact Rating (SIR): Medium

CVSS Base Score: 6.5

CVSS Vector: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

### CVE-2020-26144: Accepting plaintext A-MSDU frames that start with an RFC1042 header with EtherType EAPOL (in an encrypted network)

Security Impact Rating (SIR): Medium

CVSS Base Score: 6.5

CVSS Vector: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

### CVE-2020-26145: Accepting plaintext broadcast fragments as full frames (in an encrypted network)

Security Impact Rating (SIR): Medium

CVSS Base Score: 6.5

CVSS Vector: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

### CVE-2020-24586: Not clearing fragments from memory when (re)connecting to a network

Security Impact Rating (SIR): Medium

CVSS Base Score: 5.7

CVSS Vector: CVSS:3.1/AV:A/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N

#### CVE-2020-24588: Accepting non-SPP A-MSDU frames

Security Impact Rating (SIR): Medium

CVSS Base Score: 5.7

CVSS Vector: CVSS:3.1/AV:A/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N

#### CVE-2020-26139: Forwarding EAPOL frames even though the sender is not yet authenticated

Security Impact Rating (SIR): Medium

CVSS Base Score: 5.7

CVSS Vector: CVSS:3.1/AV:A/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:L

#### CVE-2020-26141: Not verifying the TKIP MIC of fragmented frames

Security Impact Rating (SIR): Medium

CVSS Base Score: 5.7

CVSS Vector: CVSS:3.1/AV:A/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N

#### CVE-2020-26142: Processing fragmented frames as full frames

Security Impact Rating (SIR): Medium

CVSS Base Score: 5.7

CVSS Vector: CVSS:3.1/AV:A/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N

#### CVE-2020-24587: Reassembling fragments encrypted under different keys

Security Impact Rating (SIR): Medium

CVSS Base Score: 4.8

CVSS Vector: CVSS:3.1/AV:A/AC:H/PR:N/UI:R/S:U/C:N/I:H/A:N

#### CVE-2020-26146: Reassembling encrypted fragments with non-consecutive packet numbers

Security Impact Rating (SIR): Medium

CVSS Base Score: 4.8

CVSS Vector: CVSS:3.1/AV:A/AC:H/PR:N/UI:R/S:U/C:N/I:H/A:N

#### CVE-2020-26147: Reassembling mixed encrypted/plain text fragments

Security Impact Rating (SIR): Medium

CVSS Base Score: 4.8

CVSS Vector: CVSS:3.1/AV:A/AC:H/PR:N/UI:R/S:U/C:N/I:H/A:N

## ^ Workarounds

There are no workarounds that address these vulnerabilities.

## ^ Fixed Software

For information about [fixed software releases](#), consult the Cisco bugs identified in the [Vulnerable Products](#) section of this advisory.

When [considering software upgrades](#), customers are advised to regularly consult the advisories for Cisco products, which are available from the [Cisco Security Advisories page](#), to determine exposure and a complete upgrade solution.

In all cases, customers should ensure that the devices to be upgraded contain sufficient memory and confirm that current hardware and software configurations will continue to be supported properly by the new release. If the information is not clear, customers are advised to contact the Cisco Technical Assistance Center (TAC) or their contracted maintenance providers.

## ^ Exploitation and Public Announcements

The Cisco Product Security Incident Response Team (PSIRT) is aware that proof-of-concept exploit code is available for the vulnerabilities that are described in this advisory.

The Cisco PSIRT is not aware of any malicious use of the vulnerabilities that are described in this advisory.

## ^ Source

These vulnerabilities were reported to Cisco by Dr. Mathy Vanhoef of New York University Abu Dhabi. Cisco would like to thank Dr. Vanhoef for his continued help and support during the handling of these vulnerabilities.

## ^ URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wifi-faf-22epcEWu>

## ^ Revision History

| Version | Description  | Section             | Status  | Date        |
|---------|--|---------------------|---------|-------------|
| 1.9     | Updated fixed releases.  | Vulnerable Products | Final   | 2021-DEC-15 |
| 1.8     | Updated fixed release details for Aironet 1532/AP803 products. | Vulnerable Products | Interim | 2021-OCT-05 |

[Show Complete History...](#)

## ^ Legal Disclaimer

THIS DOCUMENT IS PROVIDED ON AN "AS IS" BASIS AND DOES NOT IMPLY ANY KIND OF GUARANTEE OR WARRANTY, INCLUDING THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR USE. YOUR USE OF THE INFORMATION ON THE DOCUMENT OR MATERIALS LINKED FROM THE DOCUMENT IS AT YOUR OWN RISK. CISCO RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME.

A standalone copy or paraphrase of the text of this document that omits the distribution URL is an uncontrolled copy and may lack important information or contain factual errors. The information in this document is intended for end users of Cisco products.

▶ [Cisco Security Vulnerability Policy](#)

▶ [Subscribe to Cisco Security Notifications](#)

▶ [Related to This Advisory](#)

### Quick Links

[About Cisco](#)

[Contact Us](#)

[Careers](#)

[Connect with a partner](#)

### Resources and Legal

[Feedback](#)

[Help](#)

[Terms & Conditions](#)

[Privacy](#)

[Cookies / Do not sell or share my personal data](#)

[Accessibility](#)

[Trademarks](#)

[Supply Chain Transparency](#)

[Newsroom](#)

[Sitemap](#)



© 2026 Cisco Systems, Inc.