



CVE-2018-0441

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2018-0441
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-10-17 22:29:00 UTC
Updated	2019-10-09 23:32:00 UTC
Description	A vulnerability in the 802.11r Fast Transition feature set of Cisco IOS Access Points (APs) Software could allow an unauth

Risk And Classification

Problem Types: CWE-400

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Cisco	Access Points	All	All	All	All
Operating System	Cisco	Access Points	15.3(3)jd	All	All	All
Operating System	Cisco	Access Points	15.3(3)jd	All	All	All
Operating System	Cisco	Access Points	8.0(140.0)	All	All	All
Operating System	Cisco	Access Points	8.0(140.0)	All	All	All
Operating System	Cisco	Access Points	8.2(141.0)	All	All	All
Operating System	Cisco	Access Points	8.2(151.0)	All	All	All
Operating System	Cisco	Access Points	8.2(141.0)	All	All	All
Operating System	Cisco	Access Points	8.2(151.0)	All	All	All
Operating System	Cisco	Access Points	8.3(102.0)	All	All	All
Operating System	Cisco	Access Points	8.3(112.0)	All	All	All
Operating System	Cisco	Access Points	8.3(114.74)	All	All	All
Operating System	Cisco	Access Points	8.3(102.0)	All	All	All
Operating System	Cisco	Access Points	8.3(112.0)	All	All	All
Operating System	Cisco	Access Points	8.3(114.74)	All	All	All
Operating System	Cisco	Access Points	All	All	All	All
Operating System	Cisco	Access Points	15.3(3)jd	All	All	All

Operating System	Cisco	Access Points	8.0\140.0\)	All	All	All
Operating System	Cisco	Access Points	8.2\141.0\)	All	All	All
Operating System	Cisco	Access Points	8.2\151.0\)	All	All	All
Operating System	Cisco	Access Points	8.3\102.0\)	All	All	All
Operating System	Cisco	Access Points	8.3\112.0\)	All	All	All
Operating System	Cisco	Access Points	8.3\114.74\)	All	All	All

References

Reference

[Cisco IOS Access Points 802.11r Fast Transition Processing Bug Lets Remote Users Cause the Target Service to Crash - SecurityTracker](#)

[Cisco IOS Access Points Software 802.11r CVE-2018-0441 Denial of Service Vulnerability](#)

[Cisco IOS Access Points Software 802.11r Fast Transition Denial of Service Vulnerability](#)

[CVE Program record](#)

[NVD vulnerability detail](#)

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)