



CVE-2013-3466

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

Summary

CVE	CVE-2013-3466
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2013-08-29 12:07:00 UTC
Updated	2016-11-07 14:59:00 UTC
Description	The EAP-FAST authentication module in Cisco Secure Access Control Server (ACS) 4.x before 4.2.1.15.11, when a RADIUS

Risk And Classification

Problem Types: CWE-287

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Secure Access Control Server	4.2.1.15.0	All	All	All
Application	Cisco	Secure Access Control Server	4.2.1.15.1	All	All	All
Application	Cisco	Secure Access Control Server	4.2.1.15.2	All	All	All
Application	Cisco	Secure Access Control Server	4.2.1.15.3	All	All	All
Application	Cisco	Secure Access Control Server	4.2.1.15.4	All	All	All
Application	Cisco	Secure Access Control Server	4.2.1.15.6	All	All	All
Application	Cisco	Secure Access Control Server	4.2.1.15.7	All	All	All
Application	Cisco	Secure Access Control Server	4.2.1.15.8	All	All	All
Application	Cisco	Secure Access Control Server	4.2.1.15.9	All	All	All
Application	Cisco	Secure Access Control Server	4.2.1.15.0	All	All	All
Application	Cisco	Secure Access Control Server	4.2.1.15.1	All	All	All
Application	Cisco	Secure Access Control Server	4.2.1.15.2	All	All	All
Application	Cisco	Secure Access Control Server	4.2.1.15.3	All	All	All
Application	Cisco	Secure Access Control Server	4.2.1.15.4	All	All	All
Application	Cisco	Secure Access Control Server	4.2.1.15.6	All	All	All
Application	Cisco	Secure Access Control Server	4.2.1.15.7	All	All	All
Application	Cisco	Secure Access Control Server	4.2.1.15.8	All	All	All

Application	Cisco	Secure Access Control Server	4.2.1.15.9	All	All	All
Application	Cisco	Secure Access Control Server	All	All	All	All

References

Reference	Source
Cisco Secure Access Control Server EAP-FAST Authentication Flaw Lets Remote Users Execute Arbitrary Commands - SecurityTracker	SI
96668	O
Cisco Security Advisory: Cisco Secure Access Control Server Remote Command Execution Vulnerability	C
CVE Program record	C
NVD vulnerability detail	N

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](#)