



CVE-2019-1715

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2019-1715
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-05-03 17:29:00 UTC
Updated	2019-10-09 23:47:00 UTC
Description	A vulnerability in the Deterministic Random Bit Generator (DRBG), also known as Pseudorandom Number Generator (PRN

Risk And Classification

Problem Types: CWE-332

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Adaptive Security Appliance Device Manager	All	All	All	All
Application	Cisco	Adaptive Security Appliance Device Manager	All	All	All	All
Hardware	Cisco	Asa-5506-x	-	All	All	All
Hardware	Cisco	Asa-5506-x	-	All	All	All
Hardware	Cisco	Asa-5506h-x	-	All	All	All
Hardware	Cisco	Asa-5506h-x	-	All	All	All
Hardware	Cisco	Asa-5506w-x	-	All	All	All
Hardware	Cisco	Asa-5506w-x	-	All	All	All
Hardware	Cisco	Asa-5508-x	-	All	All	All
Hardware	Cisco	Asa-5508-x	-	All	All	All
Hardware	Cisco	Asa-5516-x	-	All	All	All
Hardware	Cisco	Asa-5516-x	-	All	All	All
Hardware	Cisco	Asa-5525-x	-	All	All	All
Hardware	Cisco	Asa-5525-x	-	All	All	All
Hardware	Cisco	Asa-5545-x	-	All	All	All
Hardware	Cisco	Asa-5545-x	-	All	All	All
Hardware	Cisco	Asa-5555-x	-	All	All	All

Hardware	Cisco	Asa-5555-x	-	All	All	All
Hardware	Cisco	Asa 5500	-	All	All	All
Hardware	Cisco	Asa 5500	-	All	All	All
Application	Cisco	Firepower Threat Defense	All	All	All	All
Application	Cisco	Firepower Threat Defense	All	All	All	All

References

Reference	Source	Link
Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software Low-Entropy Keys Vulnerability	CISCO	tools.cisco.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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