# CVE Detail – CVE-2019-1715

A vulnerability in the Deterministic Random Bit Generator (DRBG), also known as Pseudorandom Number Generator (PRNG), used in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a cryptographic collision, enabling the attacker to discover the private key of an affected device. The vulnerability is due to insufficient entropy in the DRBG when generating cryptographic keys. An attacker could exploit this vulnerability by generating a large number of cryptographic keys on an affected device and looking for collisions with target devices. A successful exploit could allow the attacker to impersonate an affected target device or to decrypt traffic secured by an affected key that is sent to or from an affected target device.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## EPSS

EPSS Score: N/A

Percentile: 0.63727

## CVSS Scoring

CVSS v3.0 Score: 5.3

Severity: MEDIUM

## Mapped CWE(s)

* CWE-332: Insufficient Entropy in PRNG

## Affected Products

* cpe:2.3:a:cisco:adaptive\_security\_appliance\_device\_manager:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:cisco:adaptive\_security\_appliance\_device\_manager:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:cisco:firepower\_threat\_defense:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:cisco:firepower\_threat\_defense:\*:\*:\*:\*:\*:\*:\*:\*