CVE-2015-6386

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2015-6386
State	PUBLISHED
Assigner	cisco
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-12-01 11:59:03 UTC
Updated	2026-05-06 22:30:45 UTC
Description	The passthrough FTP feature on Cisco Web Security Appliance (WSA) devices with software 8.0.7-142 and 8.5.1-021 allow

Risk And Classification

Primary CVSS: v2.0 5 from nvd@nist.gov

AV:N/AC:L/Au:N/C:N/I:N/A:P

Problem Types: CWE-399 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

None

Availability

Partial

AV:N/AC:L/Au:N/C:N/I:N/A:P

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Web Security Appliance	8.0.7-142	All	All	All

Application	Cisco	Web Security Appliance	8.5.1-021	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference
Cisco Web Security Appliance Native FTP Denial of Service Vulnerability
Cisco Web Security Appliance FTP Passthrough Lets Remote Users Consume Excessive CPU Resources on the Target System - SecurityTra
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.