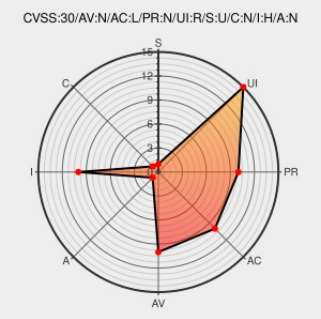
CVE-2016-6412

Published on: 09/23/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:12 PM UTC

CVE-2016-6412

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Ios from Cisco contain the following vulnerability:

The Cisco Application-hosting Framework (CAF) component in Cisco IOS 15.6(1)T1 and IOS XE, when the IOx feature set is enabled, allows man-in-the-middle attackers to trigger arbitrary downloads via crafted HTTP headers, aka Bug ID CSCuz84773.

CVE-2016-6412 has been assigned by psirt@cisco.com to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 6.5 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	NONE	HIGH	NONE

CVSS2 Score: 4.3 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
Cisco Application-Hosting Framework HTTP Header Injection Vulnerability	Vendor Advisory, tools.cisco.com, text/html	CISCO 20160921 Cisco Application-Hosting Framework HTTP Header Injection Vulnerability

Cisco IOS and IOS XE Software CVE-2016-6412 HTTP Header Injection Vulnerability	cve.report (archive) text/html	BID 93088
Cisco IOS/IOS XE Input Validation Flaw in Cisco Application-hosting Framework Lets Remote Users Force an Arbitrary File Download to the Target User - SecurityTracker	www.securitytracker.com text/html	SECTRACK 1036874

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Cisco	Ios	15.6(1)t1	All	All	All
Operating System	Cisco	Ios	15.6\(1\)t1	All	All	All
Operating System	Cisco	Ios	15.6\(1\)t1	All	All	All

cpe:2.3:o:cisco:ios:15.6(1)t1:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:15.6\(1\)t1:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:15.6\(1\)t1:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→