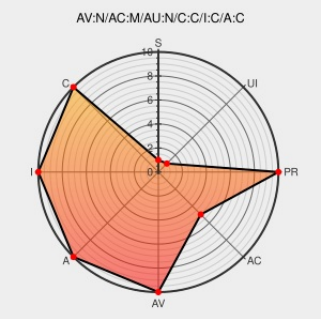
CVE-2014-2196

Published on: 05/23/2014 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:58 PM UTC

CVE-2014-2196

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



Certain versions of Wide Area Application Services from Cisco contain the following vulnerability:

Cisco Wide Area Application Services (WAAS) 5.1.1 before 5.1.1e, when SharePoint prefetch optimization is enabled, allows remote SharePoint servers to execute arbitrary code via a malformed response, aka Bug ID CSCue18479.

CVE-2014-2196 has been assigned by psirt@cisco.com to track the vulnerability

CVSS2 Score: 9.3 - HIGH

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

CVE References

Description	Tags	Link
Cisco Wide Area Application Services Buffer Overflow in Processing SharePoint Responses Lets Remote Users Execute Arbitrary Code - SecurityTracker	Third Party Advisory, VDB Entry, www.securitytracker.com, text/html	SECTRACK 1030265
Cisco Security Advisory: Cisco Wide Area Application Services Remote Code Execution Vulnerability	Vendor Advisory, tools.cisco.com, text/html	CISCO 20140521 Cisco Wide Area Application Services Remote Code Execution Vulnerability

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Wide Area Application Services	5.1.1	All	All	All
Application	Cisco	Wide Area Application Services	5.1.1	a	All	All
Application	Cisco	Wide Area Application Services	5.1.1	b	All	All
Application	Cisco	Wide Area Application Services	5.1.1	c	All	All
Application	Cisco	Wide Area Application Services	5.1.1	d	All	All
Application	Cisco	Wide Area Application Services	5.1.1	All	All	All
Application	Cisco	Wide Area Application Services	5.1.1	a	All	All
Application	Cisco	Wide Area Application Services	5.1.1	b	All	All
Application	Cisco	Wide Area Application Services	5.1.1	c	All	All
Application	Cisco	Wide Area Application Services	5.1.1	d	All	All

cpe:2.3:a:cisco:wide_area_application_services:5.1.1:*:*:*:*:*:*:*:

cpe:2.3:a:cisco:wide_area_application_services:5.1.1:a:*:*:*:*:*:*:

cpe:2.3:a:cisco:wide_area_application_services:5.1.1:b:*:*:*:*:*:*:

cpe:2.3:a:cisco:wide_area_application_services:5.1.1:c:*:*:*:*:*:*:

cpe:2.3:a:cisco:wide_area_application_services:5.1.1:d:*:*:*:*:*:*:

cpe:2.3:a:cisco:wide_area_application_services:5.1.1:*:*:*:*:*:*:*:

cpe:2.3:a:cisco:wide_area_application_services:5.1.1:a:*:*:*:*:*:*:

cpe:2.3:a:cisco:wide_area_application_services:5.1.1:b:*:*:*:*:*:*:

cpe:2.3:a:cisco:wide_area_application_services:5.1.1:c:*:*:*:*:*:*:

cpe:2.3:a:cisco:wide_area_application_services:5.1.1:d:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report