CVE-2013-3443

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

Summary

CVE	CVE-2013-3443
State	PUBLISHED
Assigner	cisco
Source Priority	CVE Program / NVD first with legacy fallback
Published	2013-08-01 13:32:30 UTC
Updated	2026-04-29 01:13:23 UTC
Description	The web service framework in Cisco WAAS Software 4.x and 5.x before 5.0.3e, 5.1.x before 5.1.1c, and 5.2.x before 5.2.1 i

Risk And Classification

Primary CVSS: v2.0 10 from nvd@nist.gov

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

Problem Types: CWE-20 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Wide Area Application Services	4.0.1	All	All	All

Application	Cisco	Wide Area Application Services	4.0.11	All	All	All
Application	Cisco	Wide Area Application Services	4.0.13	All	All	All
Application	Cisco	Wide Area Application Services	4.0.17	All	All	All
Application	Cisco	Wide Area Application Services	4.0.19	All	All	All
Application	Cisco	Wide Area Application Services	4.0.21	All	All	All
Application	Cisco	Wide Area Application Services	4.0.23	All	All	All
Application	Cisco	Wide Area Application Services	4.0.25	All	All	All
Application	Cisco	Wide Area Application Services	4.0.27	All	All	All
Application	Cisco	Wide Area Application Services	4.0.3	All	All	All
Application	Cisco	Wide Area Application Services	4.0.5	All	All	All
Application	Cisco	Wide Area Application Services	4.0.7	All	All	All
Application	Cisco	Wide Area Application Services	4.0.9	All	All	All
Application	Cisco	Wide Area Application Services	4.1.1	All	All	All
Application	Cisco	Wide Area Application Services	4.1.1	a	All	All
Application	Cisco	Wide Area Application Services	4.1.1	b	All	All
Application	Cisco	Wide Area Application Services	4.1.1	c	All	All
Application	Cisco	Wide Area Application Services	4.1.1	d	All	All
Application	Cisco	Wide Area Application Services	4.1.3	All	All	All
Application	Cisco	Wide Area Application Services	4.1.3	a	All	All
Application	Cisco	Wide Area Application Services	4.1.3	b	All	All
Application	Cisco	Wide Area Application Services	4.1.5	a	All	All
Application	Cisco	Wide Area Application Services	4.1.5	b	All	All
Application	Cisco	Wide Area Application Services	4.1.5	c	All	All
Application	Cisco	Wide Area Application Services	4.1.5	d	All	All
Application	Cisco	Wide Area Application Services	4.1.5	e	All	All
Application	Cisco	Wide Area Application Services	4.1.5	f	All	All
Application	Cisco	Wide Area Application Services	4.1.5	g	All	All
Application	Cisco	Wide Area Application Services	4.1.7	All	All	All
Application	Cisco	Wide Area Application Services	4.1.7	a	All	All
Application	Cisco	Wide Area Application Services	4.1.7	b	All	All
Application	Cisco	Wide Area Application Services	4.2.1	All	All	All
Application	Cisco	Wide Area Application Services	4.2.3	All	All	All
Application	Cisco	Wide Area Application Services	4.2.3	a	All	All
Application	Cisco	Wide Area Application Services	4.2.3	b	All	All
Application	Cisco	Wide Area Application Services	4.2.3	c	All	All
Application	Cisco	Wide Area Application Services	4.3.1	All	All	All

Application	Cisco	Wide Area Application Services	4.3.3	All	All	All
Application	Cisco	Wide Area Application Services	4.3.5	All	All	All
Application	Cisco	Wide Area Application Services	4.3.5	a	All	All
Application	Cisco	Wide Area Application Services	4.4.1	All	All	All
Application	Cisco	Wide Area Application Services	4.4.3	All	All	All
Application	Cisco	Wide Area Application Services	4.4.3	a	All	All
Application	Cisco	Wide Area Application Services	4.4.3	b	All	All
Application	Cisco	Wide Area Application Services	4.4.3	c	All	All
Application	Cisco	Wide Area Application Services	4.4.5	All	All	All
Application	Cisco	Wide Area Application Services	4.4.5	a	All	All
Application	Cisco	Wide Area Application Services	4.4.5	b	All	All
Application	Cisco	Wide Area Application Services	4.4.5	c	All	All
Application	Cisco	Wide Area Application Services	4.4.5	d	All	All
Application	Cisco	Wide Area Application Services	4.4.7	All	All	All
Application	Cisco	Wide Area Application Services	5.0.1	All	All	All
Application	Cisco	Wide Area Application Services	5.0.3	All	All	All
Application	Cisco	Wide Area Application Services	5.0.3	a	All	All
Application	Cisco	Wide Area Application Services	5.0.3	c	All	All
Application	Cisco	Wide Area Application Services	5.0.3	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	5.2	All	All	All

Vendor Declared Affected Products

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

References

Reference	Source
About Secunia Research | Flexera	af854a3a
About Secunia Research | Flexera	af854a3a
IBM X-Force Exchange	af854a3a
Cisco Wide Area Application Services CVE-2013-3443 Remote Code Execution Vulnerability	af854a3a
osvdb.org/95877	af854a3a
Cisco Wide Area Application Services Web Service Framework Bug Lets Remote Users Execute Arbitrary Code - SecurityTracker	af854a3a

Cisco Security Advisory: Cisco WAAS Central Manager Remote Code Execution Vulnerability	af854a3a
CVE Program record	CVE.OR
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.