CVE-2006-3291

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

Summary

CVE	CVE-2006-3291
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-06-28 23:05:00 UTC
Updated	2017-07-20 01:32:00 UTC
Description	The web interface on Cisco IOS 12.3(8)JA and 12.3(8)JA1, as used on the Cisco Wireless Access Point and Wireless Bridg

Risk And Classification

Problem Types: CWE-16

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Cisco	Ios	12.3(8)ja	All	All	All
Operating System	Cisco	Ios	12.3(8)ja1	All	All	All
Operating System	Cisco	Ios	12.3\(8\)ja	All	All	All
Operating System	Cisco	Ios	12.3\(8\)ja1	All	All	All
Operating System	Cisco	Ios	12.3\(8\)ja	All	All	All
Operating System	Cisco	Ios	12.3\(8\)ja1	All	All	All

References

Reference	Source	L
IBM X-Force Exchange	XF	e
26878	OSVDB	v
Cisco Access Point Web Interface Authorization Bypass Vulnerability	BID	v
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	v
SecurityTracker.com Archives - Cisco Access Point Configuration Error May Let Remote Users Gain Administrative Access	SECTRACK	s
Cisco Wireless Access Point Web Management Vulnerability - Advisories - Secunia	SECUNIA	s
US-CERT Vulnerability Note VU#544484	CERT-VN	v
Cisco - Networking, Cloud, and Cybersecurity Solutions	CISCO	v

CVE Program record	CVE.ORG	v
NVD vulnerability detail	NVD	r

No vendor comments have been submitted for this CVE.

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