CVE-2004-2443

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

Summary

CVE	CVE-2004-2443
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2004-12-31 05:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	Jaws 0.3 allows remote attackers to bypass authentication and via an HTTP request to admin.php with the logged cookie se

Risk And Classification

Primary CVSS: v2.0 7.5 from nvd@nist.gov

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

Problem Types: NVD-CWE-Other | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Jaws	Jaws	0.2	All	All	All

Application	Jaws	Jaws	0.3	All	All	All

Vendor Declared Affected Products

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

References

Reference	Source	L
archives.neohapsis.com/archives/fulldisclosure/2004-07/0226.html	af854a3a-2127-422b-91ae-364da2661108	a
JAWS Multiple Input Validation Vulnerabilities	af854a3a-2127-422b-91ae-364da2661108	w
Jaws Errors Let Remote Users View Files and Gain Administrative Access - SecurityTracker	af854a3a-2127-422b-91ae-364da2661108	s
www.osvdb.org/7724	af854a3a-2127-422b-91ae-364da2661108	w
IBM X-Force Exchange	af854a3a-2127-422b-91ae-364da2661108	e
CVE Program record	CVE.ORG	w
NVD vulnerability detail	NVD	n

No vendor comments have been submitted for this CVE.

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