CVE-2005-3252

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2005-3252
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2005-10-18 21:02:00 UTC
Updated	2011-03-08 02:26:00 UTC
Description	Stack-based buffer overflow in the Back Orifice (BO) preprocessor for Snort before 2.4.3 allows remote attackers to execute

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sourcefire	Snort	2.4.0	All	All	All
Application	Sourcefire	Snort	2.4.1	All	All	All
Application	Sourcefire	Snort	2.4.2	All	All	All
Application	Sourcefire	Snort	2.4.0	All	All	All
Application	Sourcefire	Snort	2.4.1	All	All	All
Application	Sourcefire	Snort	2.4.2	All	All	All

References

Reference	Source
US-CERT Vulnerability Note VU#175500	CERT-VN
Secunia - Advisories - Nortel Threat Protection System Back Orifice Pre-Processor Buffer Overflow	SECUNIA
Neohapsis Archives - Full Disclosure List - #0010 - [Full-disclosure] Snort Back Orifice Preprocessor Exploit (Win32 targets)	FULLDISC
Secunia - Advisories - Snort Back Orifice Pre-Processor Buffer Overflow Vulnerability	SECUNIA
Nortel: Technical Support	CONFIRM
US-CERT Technical Cyber Security Alert TA05-291A -- Snort Back Orifice Preprocessor Buffer Overflow	CERT
Secunia - Advisories - SUSE Updates for Multiple Packages	SECUNIA
Just a moment...	CONFIRM

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN
Snort Back Orifice Preprocessor Remote Stack Buffer Overflow Vulnerability	BID
Neohapsis Archives - Full Disclosure List - #0505 - [Full-disclosure] Snort's BO pre-processor exploit	FULLDISC
20034	OSVDB
Nortel: Technical Support	CONFIRM
SecurityTracker.com Archives - Snort Buffer Overflow in Back Orifice Preprocessor Lets Remote Users Execute Arbitrary Code	SECTRACK
Internet Security Systems -	ISS
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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