



CVE-2007-4872

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2007-4872
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-09-27 19:17:00 UTC
Updated	2026-04-23 00:35:47 UTC
Description	SimpNews 2.41.03 allows remote attackers to obtain sensitive information via (1) an invalid lang parameter to admin/index.

Risk And Classification

Primary CVSS: v2.0 5 from nvd@nist.gov

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

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

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

None

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Simplenews	Simplenews	2.41.03	All	All	All

Vendor Declared Affected Products				
Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified
References				
Reference			Source	Link
SecurityFocus			af854a3a-2127-422b-91ae-364da2661108	www.sec
SimpNews version 2.41.03 Multiple Path Disclosure Vulnerabilities - CXSecurity.com			af854a3a-2127-422b-91ae-364da2661108	securityre
[Full-disclosure] SimpNews version 2.41.03 Multiple Path Disclosure Vulnerabilities			af854a3a-2127-422b-91ae-364da2661108	lists.grok
netVigilance, Inc. - Security Advisory 68			af854a3a-2127-422b-91ae-364da2661108	www.net
IBM X-Force Exchange			af854a3a-2127-422b-91ae-364da2661108	exchange
forum.boesch-it.de/viewtopic.php			af854a3a-2127-422b-91ae-364da2661108	forum.bo
osvdb.org/43541			af854a3a-2127-422b-91ae-364da2661108	osvdb.org
osvdb.org/43540			af854a3a-2127-422b-91ae-364da2661108	osvdb.org
osvdb.org/43543			af854a3a-2127-422b-91ae-364da2661108	osvdb.org
osvdb.org/43542			af854a3a-2127-422b-91ae-364da2661108	osvdb.org
CVE Program record			CVE.ORG	www.cve
NVD vulnerability detail			NVD	nvd.nist.g
No vendor comments have been submitted for this CVE.				
There are currently no legacy QID mappings associated with this CVE.				