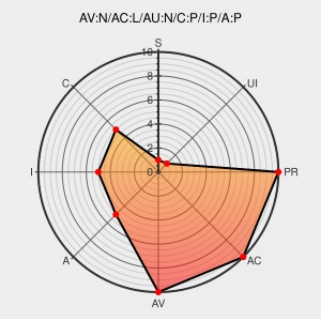
CVE-2006-0994

Published on: 05/10/2006 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:05 PM UTC

CVE-2006-0994

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Sophos Anti-virus from Sophos contain the following vulnerability:

Multiple Sophos Anti-Virus products, including Anti-Virus for Windows 5.x before 5.2.1 and 4.x before 4.05, when cabinet file inspection is enabled, allows remote attackers to execute arbitrary code via a CAB file with "invalid folder count values," which leads to heap corruption.

CVE-2006-0994 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 7.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Sophos Anti-Virus CAB File Scanning Remote Heap Overflow Vulnerability	Third Party Advisory, VDB Entry, cve.report (archive), text/html	BID 17876
IBM X-Force Exchange	Third Party Advisory, VDB Entry, exchange.xforce.ibmcloud.com, text/html	XF sophos-cab-parsing-bo(26305)
SecurityFocus	www.securityfocus.com, text/html	BUGTRAQ 20060508 ZDI-06-012: Sophos Anti-Virus CAB Unpacking Code Execution Vulnerability
ZDI-06-012 | Zero Day Initiative	Third Party Advisory, VDB Entry, www.zerodayinitiative.com	MISC www.zerodayinitiative.com/advisories/ZDI-06-012.html

	text/html	
[Full-disclosure] ZDI-06-012: Sophos Anti-Virus CAB Unpacking Code Execution Vulnerability	Third Party Advisory web.archive.org text/html Inactive Link Not Archived	FULLDISC 20060508 ZDI-06-012: Sophos Anti-Virus CAB Unpacking Code Execution Vulnerability
Sophos Anti-Virus Cabinet File Processing Memory Corruption - Advisories - Secunia	Third Party Advisory web.archive.org text/html	SECUNIA 20028
SecurityReason	Third Party Advisory securityreason.com text/html	SREASON 869
Webmail : Solution de messagerie professionnelle - OVHcloud-OVH	Permissions Required Third Party Advisory www.vupen.com text/html	VUPEN ADV-2006-1730
SecurityTracker.com Archives - Sophos Anti-Virus Buffer Overflow in Parsing CAB Headers Lets Remote Users Execute Arbitrary Code	Third Party Advisory VDB Entry securitytracker.com text/html	SECTRACK 1016041

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sophos	Sophos Anti-virus	All	All	All	All
Application	Sophos	Sophos Anti-virus	All	All	All	All

cpe:2.3:a:sophos:sophos_anti-virus:*:*:*:*:*:*:*:*:

cpe:2.3:a:sophos:sophos_anti-virus:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report