

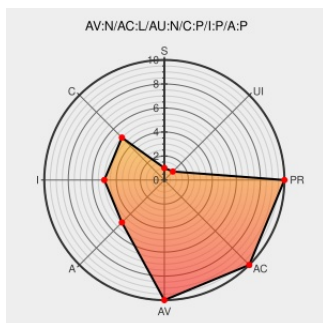


# CVE-2006-0994

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 [M](#) [cve@mitre.org](mailto:cve@mitre.org) to track the vulnerability

CVSS2 Score: **7.5 - HIGH**

Access  
Vector

**NETWORK**

Access  
Complexity

**LOW**

Authentication

**NONE**

Confidentiality  
Impact

**PARTIAL**

Integrity  
Impact

**PARTIAL**

Availability  
Impact

**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](#)

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

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to [comment@cve.report](mailto:comment@cve.report).

There are currently no QIDs associated with this CVE

## Known Affected Configurations (CPE V2.3)

| Type                                              | Vendor                 | Product                           | Version | Update | Edition | Language |
|---------------------------------------------------|------------------------|-----------------------------------|---------|--------|---------|----------|
| Application                                       | <a href="#">Sophos</a> | <a href="#">Sophos Anti-virus</a> | All     | All    | All     | All      |
| Application                                       | <a href="#">Sophos</a> | <a href="#">Sophos Anti-virus</a> | 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→

