



Published on: 04/23/2004 04:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:09 PM UTC

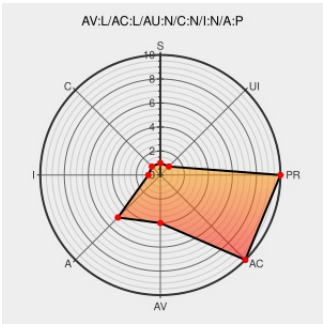
CVE-2004-1356

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Solaris](#) from [Sun](#) contain the following vulnerability:

Unknown vulnerability in the sendfilev function in Sun Solaris 8 and 9 allows local users to cause a denial of service (system panic) via unknown vectors.

CVE-2004-1356 has been assigned by  cve@mitre.org to track the vulnerability

CVSS2 Score: 2.1 - LOW

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
No Description Provided	Patch www.osvdb.org Inactive Link Not Archived	 OSVDB 5619
AusCERT - ESB-2004.0307 -- Sun(sm) Alert Notification - Sun Alert ID: 57470 -- Security Vulnerability With the Extended Library Function sendfilev(3EXT)	Patch Vendor Advisory web.archive.org text/html Inactive Link Not Archived	 AUSCERT ESB-2004.0307
No Description Provided	Patch Vendor Advisory sunsolve.sun.com Inactive Link Not Archived	 SUNALERT 57470

Repository / Oval Repository	oval.cisecurity.org text/html	 OVAL oval:org.mitre.oval:def:1684
Sun Solaris SendFileV Local Denial Of Service Vulnerability	Patch cve.report (archive) text/html	 BID 10202
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	 XF solaris-sendfilev-dos(15946)
Secunia - Advisories - Sun Solaris "sendfile()" Extended Library Function Denial of Service	Patch Vendor Advisory web.archive.org text/html	 SECUNIA 11457

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.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Sun	Solaris	8.0	All	x86	All
Operating System	Sun	Solaris	9.0	All	sparc	All
Operating System	Sun	Solaris	9.0	All	x86	All
Operating System	Sun	Solaris	8.0	All	x86	All
Operating System	Sun	Solaris	9.0	All	sparc	All
Operating System	Sun	Solaris	9.0	All	x86	All
Operating System	Sun	Sunos	5.8	All	All	All
Operating System	Sun	Sunos	5.8	All	All	All
cpe:2.3:o:sun:solaris:8.0:*:x86:****:*:						
cpe:2.3:o:sun:solaris:9.0:*:sparc:****:*:						
cpe:2.3:o:sun:solaris:9.0:*:x86:****:*:						
cpe:2.3:o:sun:solaris:8.0:*:x86:****:*:						
cpe:2.3:o:sun:solaris:9.0:*:sparc:****:*:						
cpe:2.3:o:sun:solaris:9.0:*:x86:****:*:						

cpe:2.3:o:sun:sunos:5.8:*:*:*:*:*:

cpe:2.3:o:sun:sunos:5.8:*:*:*:*:*:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)

© [CVE.report](#) 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)