



Published on: 04/13/2006 12:00:00 AM UTC

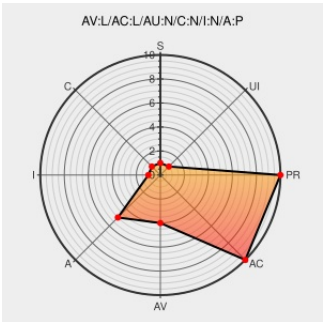
Last Modified on: 03/23/2021 11:25:00 PM UTC

CVE-2006-1780

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF 

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

The Bourne shell (sh) in Solaris 8, 9, and 10 allows local users to cause a denial of service (sh crash) via an unspecified attack vector that causes sh processes to crash during creation of temporary files.

CVE-2006-1780 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
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com text/html	VUPEN ADV-2006-1333
ASA-2006-122 (SUN 102113, 102282, 102292, 102302)	support.avaya.com text/html	CONFIRM support.avaya.com/elmodocs2/security/ASA-2006-122.htm
#102282: Security Vulnerability May Allow 'sh' Process to be Crashed Causing a Denial of Service	web.archive.org text/html Inactive Link Not Archived	SUNALERT 102282
Sun Solaris SH(1) Local Denial of Service Vulnerability	cve.report (archive) text/html	BID 17478
Avaya CMS / IR Sun Solaris LDAP2 and "sh" Vulnerabilities - Advisories - Secunia	web.archive.org text/html	SECUNIA 21493

Repository / Oval Repository	oval.cisecurity.org text/html	 OVAL oval.org/mitre.oval:def:881
Sun Solaris "sh" Process Denial of Service Vulnerability - Advisories - Secunia	Patch Vendor Advisory web.archive.org text/html	 SECUNIA 19627
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	 XF solaris-sh-dos(25744)
Solaris Bug in sh Temporary File Creation Lets Local Users Deny Service - SecurityTracker	securitytracker.com text/html	 SECTRACK 1015902

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	10.0	All	sparc	All
Operating System	Sun	Solaris	9.0	All	sparc	All
Operating System	Sun	Solaris	10.0	All	sparc	All
Operating System	Sun	Solaris	9.0	All	sparc	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:10.0*:sparc:*****:						
cpe:2.3:o:sun:solaris:9.0*:sparc:*****:						
cpe:2.3:o:sun:solaris:10.0*:sparc:*****:						
cpe:2.3:o:sun:solaris:9.0*:sparc:*****:						
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

© [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](#)