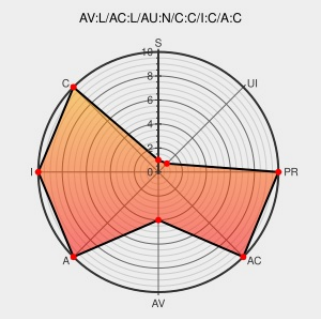
CVE-2002-1296

Published on: 12/23/2002 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:02 PM UTC

CVE-2002-1296

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



Certain versions of Solaris from Sun contain the following vulnerability:

Directory traversal vulnerability in priocntl system call in Solaris does allows local users to execute arbitrary code via ".." sequences in the pc_clname field of a pcinfo_t structure, which cause priocntl to load a malicious kernel module.

CVE-2002-1296 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 7.2 - HIGH

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
'Solaris priocntl exploit' - MARC	marc.info text/x-c	BUGTRAQ 20021127 Solaris priocntl exploit
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:3637
Solaris priocntl() System Call Local Root Vulnerability	cve.report (archive) text/html	BID 6262
Free Sun Alert Notifications Article 49131	Patch Vendor Advisory web.archive.org text/html Inactive Link Not Archived	CONFIRM sunsolve.Sun.COM/pub-cgi/retrieve.pl?doc=fsalert/49131
CERT/CC Vulnerability Note VU#683673	Patch Third Party Advisory	CERT-VN VU#683673

	US Government Resource www.kb.cert.org text/html	
ISS X-Force Database: solaris-priocntl-pcclname-modules (10717): Solaris priocntl(2) pc_clname argument could allow an attacker to load modules	Vendor Advisory web.archive.org text/html Inactive Link Not Archived	XF solaris-priocntl-pcclname-modules(10717)

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	2.6	All	All	All
Operating System	Sun	Solaris	7.0	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	2.6	All	All	All
Operating System	Sun	Solaris	7.0	All	x86	All
Operating System	Sun	Solaris	8.0	All	x86	All
Operating System	Sun	Solaris	9.0	All	sparc	All
Operating System	Sun	Sunos	5.5.1	All	All	All
Operating System	Sun	Sunos	5.7	All	All	All
Operating System	Sun	Sunos	5.8	All	All	All
Operating System	Sun	Sunos	5.5.1	All	All	All
Operating System	Sun	Sunos	5.7	All	All	All
Operating System	Sun	Sunos	5.8	All	All	All

cpe:2.3:o:sun:solaris:2.6:*:*:*:*:*:*:*

cpe:2.3:o:sun:solaris:7.0:*: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:2.6:*:*:*:*:*:*:*:

cpe:2.3:o:sun:solaris:7.0:*:x86:*:*:*:*:*:

cpe:2.3:o:sun:solaris:8.0:*:x86:*:*:*:*:*:

cpe:2.3:o:sun:solaris:9.0:*:sparc:*:*:*:*:*:

cpe:2.3:o:sun:sunos:5.5.1:*:*:*:*:*:*:*:

cpe:2.3:o:sun:sunos:5.7:*:*:*:*:*:*:*:

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

cpe:2.3:o:sun:sunos:5.5.1:*:*:*:*:*:*:*:

cpe:2.3:o:sun:sunos:5.7:*:*:*:*:*:*:*:

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 registred 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