

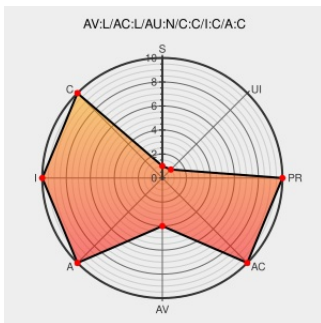


CVE-2003-1057

Published on: 12/08/2003 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:43 PM UTC

CVE-2003-1057

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

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

Unknown vulnerability in CDE Print Viewer (dtprintinfo) for Sun Solaris 2.6 through 9 may allow local users to execute arbitrary code.

CVE-2003-1057 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **7.2 - HIGH**

Access
Vector

LOCAL

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

COMPLETE

Integrity
Impact

COMPLETE

Availability
Impact

COMPLETE

CVE References

Description

Tags

Link

O-035: Sun 'dtprintinfo(1)' CDE Print Viewer Vulnerability

Patch

Vendor Advisory

web.archive.org

text/html

Inactive Link Not Archived

[CIAC O-035](#)

#57441: Security Vulnerability in dtprintinfo java.lang.NullPointerException

Patch

Vendor Advisory

web.archive.org

text/html

Inactive Link Not Archived

[SUNALERT 57441](#)

Secunia - Advisories - Sun Solaris dtprintinfo Privilege Escalation Vulnerability

Patch

Vendor Advisory

web.archive.org

text/html

[SECUNIA 10384](#)

IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	 XF cde-dtprintinfo-gain-privileges(13914)
No Description Provided	Patch Vendor Advisory www.osvdb.org	 OSVDB 2924
	Inactive Link Not Archived	
CDE DTPrintInfo Home Environment Variable Buffer Overflow Vulnerability	cve.report (archive) text/html	 BID 9170
AusCERT - ESB-2003.0844 -- Sun(sm) Alert Notification - Sun Alert ID: 57441 -- Security Vulnerability in dtprintinfo(1)	Patch Vendor Advisory web.archive.org text/html	 AUSCERT ESB-2003.0844
	Inactive Link Not Archived	

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	9.0	All	x86	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	Solaris	9.0	All	x86	All
Operating System	Sun	Sunos	-	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	-	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:9.0:*:x86:*:*:*:*:						
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:9.0:*:x86:*:*:*:*:						
cpe:2.3:o:sun:sunos:-:*:*:*:*:*:						
cpe:2.3:o:sun:sunos:5.7:*:*:*:*:*:						
cpe:2.3:o:sun:sunos:5.8:*:*:*:*:*:						
cpe:2.3:o:sun:sunos:-:*:*:*:*:*:						
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

[site](#). This site includes MITRE data granted under the following [license](#).

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