



CVE-2002-0679

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2002-0679
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2002-09-05 04:00:00 UTC
Updated	2018-10-30 16:26:00 UTC
Description	Buffer overflow in Common Desktop Environment (CDE) ToolTalk RPC database server (rpc.ttdbserverd) allows remote att

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Caldera	Openunix	8.0	All	All	All
Operating System	Caldera	Openunix	8.0	All	All	All
Application	Caldera	Unixware	7.0	All	All	All
Application	Caldera	Unixware	7.1.0	All	All	All
Application	Caldera	Unixware	7.1.1	All	All	All
Application	Caldera	Unixware	7.0	All	All	All
Application	Caldera	Unixware	7.1.0	All	All	All
Application	Caldera	Unixware	7.1.1	All	All	All
Operating System	Compaq	Tru64	4.0f	All	All	All
Operating System	Compaq	Tru64	4.0g	All	All	All
Operating System	Compaq	Tru64	5.0a	All	All	All
Operating System	Compaq	Tru64	5.1	All	All	All
Operating System	Compaq	Tru64	5.1a	All	All	All
Operating System	Compaq	Tru64	4.0f	All	All	All
Operating System	Compaq	Tru64	4.0g	All	All	All
Operating System	Compaq	Tru64	5.0a	All	All	All
Operating System	Compaq	Tru64	5.1	All	All	All

Operating System	Compaq	Tru64	5.1a	All	All	All
Operating System	Hp	Hp-ux	10.10	All	All	All
Operating System	Hp	Hp-ux	10.20	All	All	All
Operating System	Hp	Hp-ux	10.24	All	All	All
Operating System	Hp	Hp-ux	11.00	All	All	All
Operating System	Hp	Hp-ux	11.11	All	All	All
Operating System	Hp	Hp-ux	10.10	All	All	All
Operating System	Hp	Hp-ux	10.20	All	All	All
Operating System	Hp	Hp-ux	10.24	All	All	All
Operating System	Hp	Hp-ux	11.00	All	All	All
Operating System	Hp	Hp-ux	11.11	All	All	All
Operating System	lbn	Aix	4.3.3	All	All	All
Operating System	lbn	Aix	5.1	All	All	All
Operating System	lbn	Aix	4.3.3	All	All	All
Operating System	lbn	Aix	5.1	All	All	All
Operating System	Sun	Solaris	2.6	All	All	All
Operating System	Sun	Solaris	9.0	All	sparc	All
Operating System	Sun	Solaris	2.6	All	All	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
Application	Xi Graphics	Dextop	2.1	All	All	All
Application	Xi Graphics	Dextop	2.1	All	All	All

References

Reference

HPSBUX0207-199

Repository / Oval Repository

Search results

Free Sun Alert Notifications Article 46366

CERT/CC Vulnerability Note VU#387387

Search results

CERT Advisory CA-2002-26 Buffer Overflow in CDE ToolTalk

Multiple Vendor CDE ToolTalk Database Server Heap Corruption Vulnerability

ISS X-Force Database: tooltalk-ttdbserverd-ttcreatefile-bo (9822): CDE ToolTalk rpc.ttdbserverd _TT_CREATE_FILE() heap buffer overflow

20020812 ENTERCEPT RICOCHET ADVISORY: Multi-Vendor CDE ToolTalk Database

CVE Program record

NVD vulnerability detail



No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

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](#)