



# CVE-2001-0117

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

## Summary

<b>CVE</b>	CVE-2001-0117
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2001-03-12 05:00:00 UTC
<b>Updated</b>	2017-10-10 01:29:00 UTC
<b>Description</b>	sdiff 2.7 in the diffutils package allows local users to overwrite files via a symlink attack.

## Risk And Classification

**Problem Types:** NVD-CWE-Other

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Immunix</a>	<a href="#">Immunix</a>	7.0_beta	All	All	All
Application	<a href="#">Immunix</a>	<a href="#">Immunix</a>	7.0_beta	All	All	All
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrake Linux</a>	6.0	All	All	All
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrake Linux</a>	6.1	All	All	All
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrake Linux</a>	7.0	All	All	All
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrake Linux</a>	7.1	All	All	All
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrake Linux</a>	7.2	All	All	All
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrake Linux</a>	6.0	All	All	All
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrake Linux</a>	6.1	All	All	All
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrake Linux</a>	7.0	All	All	All
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrake Linux</a>	7.1	All	All	All
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrake Linux</a>	7.2	All	All	All
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrake Linux Corporate Server</a>	1.0.1	All	All	All
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrake Linux Corporate Server</a>	1.0.1	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Linux</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Linux</a>	7.0	All	All	All
Operating System	<a href="#">Trustix</a>	<a href="#">Secure Linux</a>	1.1	All	All	All

Operating System	<a href="#">Trustix</a>	<a href="#">Secure Linux</a>	1.2	All	All	All
Operating System	<a href="#">Trustix</a>	<a href="#">Secure Linux</a>	1.1	All	All	All
Operating System	<a href="#">Trustix</a>	<a href="#">Secure Linux</a>	1.2	All	All	All

## References

Reference	Source	Link	Tags
'Immunix OS Security update for lots of temp file problems' - MARC	BUGTRAQ	<a href="#">marc.info</a>	
CERT/CC Vulnerability Note VU#579928	CERT-VN	<a href="#">www.kb.cert.org</a>	US Government Reso
sdiff /tmp File Race Condition Vulnerability	BID	<a href="#">www.securityfocus.com</a>	Patch, Vendor Advisor
MDKSA-2001:008-1	MANDRAKE	<a href="#">www.linux-mandrake.com</a>	Patch
IBM X-Force Exchange	XF	<a href="#">exchange.xforce.ibmcloud.com</a>	
redhat.com   Red Hat Support	REDHAT	<a href="#">www.redhat.com</a>	
IMNX-2000-70-028-01	IMMUNIX	<a href="#">download.immunix.org</a>	
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>	canonical, analysis

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](#)