



# CVE-2001-0170

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

## Summary

<b>CVE</b>	CVE-2001-0170
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2001-03-26 05:00:00 UTC
<b>Updated</b>	2017-10-10 01:29:00 UTC
<b>Description</b>	glibc 2.1.9x and earlier does not properly clear the RESOLV_HOST_CONF, HOSTALIASES, or RES_OPTIONS environme

## Risk And Classification

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

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Conectiva</a>	<a href="#">Linux</a>	4.0	All	All	All
Operating System	<a href="#">Conectiva</a>	<a href="#">Linux</a>	4.0es	All	All	All
Operating System	<a href="#">Conectiva</a>	<a href="#">Linux</a>	4.1	All	All	All
Operating System	<a href="#">Conectiva</a>	<a href="#">Linux</a>	4.2	All	All	All
Operating System	<a href="#">Conectiva</a>	<a href="#">Linux</a>	5.0	All	All	All
Operating System	<a href="#">Conectiva</a>	<a href="#">Linux</a>	5.1	All	All	All
Operating System	<a href="#">Conectiva</a>	<a href="#">Linux</a>	6.0	All	All	All
Operating System	<a href="#">Conectiva</a>	<a href="#">Linux</a>	ecommerce	All	All	All
Operating System	<a href="#">Conectiva</a>	<a href="#">Linux</a>	graficas	All	All	All
Operating System	<a href="#">Conectiva</a>	<a href="#">Linux</a>	4.0	All	All	All
Operating System	<a href="#">Conectiva</a>	<a href="#">Linux</a>	4.0es	All	All	All
Operating System	<a href="#">Conectiva</a>	<a href="#">Linux</a>	4.1	All	All	All
Operating System	<a href="#">Conectiva</a>	<a href="#">Linux</a>	4.2	All	All	All
Operating System	<a href="#">Conectiva</a>	<a href="#">Linux</a>	5.0	All	All	All
Operating System	<a href="#">Conectiva</a>	<a href="#">Linux</a>	5.1	All	All	All
Operating System	<a href="#">Conectiva</a>	<a href="#">Linux</a>	6.0	All	All	All
Operating System	<a href="#">Conectiva</a>	<a href="#">Linux</a>	ecommerce	All	All	All

Operating System	<a href="#">Conectiva</a>	<a href="#">Linux</a>	graficas	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	2.3	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	2.3	All	All	All
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="#">Redhat</a>	<a href="#">Linux</a>	7.0	All	alpha	All
Operating System	<a href="#">Redhat</a>	<a href="#">Linux</a>	7.0	All	i386	All
Operating System	<a href="#">Redhat</a>	<a href="#">Linux</a>	7.0	All	alpha	All
Operating System	<a href="#">Redhat</a>	<a href="#">Linux</a>	7.0	All	i386	All

## References

Reference	Source
<a href="#">glibc RESOLV_HOST_CONF File Read Access Vulnerability</a>	BID
<a href="#">IBM X-Force Exchange</a>	XF
<a href="#">Support</a>	RE
<a href="#">Neohapsis Archives - Bugtraq - [slackware-security] glibc 2.2 local vulnerability on setuid binaries - From security@SLACKWARE.COM</a>	BU
<a href="#">Neohapsis Archives - Bugtraq - Glibc Local Root Exploit - From csteven@NEWHOPE.TERRAPLEX.COM</a>	BU
<a href="#">CVE Program record</a>	CV
<a href="#">NVD vulnerability detail</a>	NV

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](#)