



# CVE-1999-1386

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

## Summary

<b>CVE</b>	CVE-1999-1386
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	1999-12-31 05:00:00 UTC
<b>Updated</b>	2024-01-26 16:54:00 UTC
<b>Description</b>	Perl 5.004_04 and earlier follows symbolic links when running with the -e option, which allows local users to overwrite arbitrary files.

## Risk And Classification

**Problem Types:** CWE-59

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Larry Wall	Perl	All	All	All	All
Application	Perl	Perl	All	All	All	All

## References

Reference	Source	Link	Tags
ISS X-Force Database: perl-e-tmp-symlink (7243): Perl -e command /tmp file symlink attack	XF	<a href="http://www.iss.net">www.iss.net</a>	
redhat.com   Red Hat Support	CONFIRM	<a href="http://www.redhat.com">www.redhat.com</a>	
'another /tmp race: `perl -e` opens temp file not safely' - MARC	BUGTRAQ	<a href="http://marc.info">marc.info</a>	
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canonical, and

No vendor comments have been submitted for this CVE.

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

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](#)**