



# CVE-2005-0156

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2005-0156
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2005-02-07 05:00:00 UTC
<b>Updated</b>	2023-11-07 01:57:00 UTC
<b>Description</b>	Buffer overflow in the PerlIO implementation in Perl 5.8.0, when installed with setuid support (sperl), allows local users to e

## 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="#">ibm</a>	<a href="#">Aix</a>	5.2	All	All	All
Operating System	<a href="#">ibm</a>	<a href="#">Aix</a>	5.3	All	All	All
Operating System	<a href="#">ibm</a>	<a href="#">Aix</a>	5.2	All	All	All
Operating System	<a href="#">ibm</a>	<a href="#">Aix</a>	5.3	All	All	All
Application	<a href="#">Larry Wall</a>	<a href="#">Perl</a>	5.8.0	All	All	All
Application	<a href="#">Larry Wall</a>	<a href="#">Perl</a>	5.8.1	All	All	All
Application	<a href="#">Larry Wall</a>	<a href="#">Perl</a>	5.8.3	All	All	All
Application	<a href="#">Larry Wall</a>	<a href="#">Perl</a>	5.8.4	All	All	All
Application	<a href="#">Larry Wall</a>	<a href="#">Perl</a>	5.8.4.1	All	All	All
Application	<a href="#">Larry Wall</a>	<a href="#">Perl</a>	5.8.4.2	All	All	All
Application	<a href="#">Larry Wall</a>	<a href="#">Perl</a>	5.8.4.2.3	All	All	All
Application	<a href="#">Larry Wall</a>	<a href="#">Perl</a>	5.8.4.3	All	All	All
Application	<a href="#">Larry Wall</a>	<a href="#">Perl</a>	5.8.4.4	All	All	All
Application	<a href="#">Larry Wall</a>	<a href="#">Perl</a>	5.8.4.5	All	All	All
Application	<a href="#">Larry Wall</a>	<a href="#">Perl</a>	5.8.0	All	All	All
Application	<a href="#">Larry Wall</a>	<a href="#">Perl</a>	5.8.1	All	All	All
Application	<a href="#">Larry Wall</a>	<a href="#">Perl</a>	5.8.3	All	All	All

Application	Larry Wall	Perl	5.8.4	All	All	All
Application	Larry Wall	Perl	5.8.4.1	All	All	All
Application	Larry Wall	Perl	5.8.4.2	All	All	All
Application	Larry Wall	Perl	5.8.4.2.3	All	All	All
Application	Larry Wall	Perl	5.8.4.3	All	All	All
Application	Larry Wall	Perl	5.8.4.4	All	All	All
Application	Larry Wall	Perl	5.8.4.5	All	All	All
Operating System	Redhat	Enterprise Linux	3.0	All	advanced_server	All
Operating System	Redhat	Enterprise Linux	3.0	All	enterprise_server	All
Operating System	Redhat	Enterprise Linux	3.0	All	workstation_server	All
Operating System	Redhat	Enterprise Linux	3.0	All	advanced_server	All
Operating System	Redhat	Enterprise Linux	3.0	All	enterprise_server	All
Operating System	Redhat	Enterprise Linux	3.0	All	workstation_server	All
Operating System	Redhat	Enterprise Linux Desktop	3.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	3.0	All	All	All
Operating System	Redhat	Fedora Core	core_3.0	All	All	All
Operating System	Redhat	Fedora Core	core_3.0	All	All	All
Application	Sgi	Propack	3.0	All	All	All
Application	Sgi	Propack	3.0	All	All	All
Operating System	Suse	Suse Linux	8.0	All	All	All
Operating System	Suse	Suse Linux	8.0	All	i386	All
Operating System	Suse	Suse Linux	8.1	All	All	All
Operating System	Suse	Suse Linux	8.2	All	All	All
Operating System	Suse	Suse Linux	9.0	All	All	All
Operating System	Suse	Suse Linux	9.0	All	x86_64	All
Operating System	Suse	Suse Linux	9.1	All	All	All
Operating System	Suse	Suse Linux	9.2	All	All	All
Operating System	Suse	Suse Linux	8.0	All	All	All
Operating System	Suse	Suse Linux	8.0	All	i386	All
Operating System	Suse	Suse Linux	8.1	All	All	All
Operating System	Suse	Suse Linux	8.2	All	All	All
Operating System	Suse	Suse Linux	9.0	All	All	All
Operating System	Suse	Suse Linux	9.0	All	x86_64	All
Operating System	Suse	Suse Linux	9.1	All	All	All
Operating System	Suse	Suse Linux	9.2	All	All	All

Operating System	<a href="#">Trustix</a>	<a href="#">Secure Linux</a>	1.5	All	All	All
Operating System	<a href="#">Trustix</a>	<a href="#">Secure Linux</a>	2.0	All	All	All
Operating System	<a href="#">Trustix</a>	<a href="#">Secure Linux</a>	2.1	All	All	All
Operating System	<a href="#">Trustix</a>	<a href="#">Secure Linux</a>	2.2	All	All	All
Operating System	<a href="#">Trustix</a>	<a href="#">Secure Linux</a>	1.5	All	All	All
Operating System	<a href="#">Trustix</a>	<a href="#">Secure Linux</a>	2.0	All	All	All
Operating System	<a href="#">Trustix</a>	<a href="#">Secure Linux</a>	2.1	All	All	All
Operating System	<a href="#">Trustix</a>	<a href="#">Secure Linux</a>	2.2	All	All	All
Operating System	<a href="#">Ubuntu</a>	<a href="#">Ubuntu Linux</a>	4.1	All	ia64	All
Operating System	<a href="#">Ubuntu</a>	<a href="#">Ubuntu Linux</a>	4.1	All	ppc	All
Operating System	<a href="#">Ubuntu</a>	<a href="#">Ubuntu Linux</a>	4.1	All	ia64	All
Operating System	<a href="#">Ubuntu</a>	<a href="#">Ubuntu Linux</a>	4.1	All	ppc	All

## References

Reference	Source	Link	Tags
Secunia - Advisories - Perl "PERLIO_DEBUG" Privilege Escalation Vulnerabilities	SECUNIA	<a href="https://secunia.com">secunia.com</a>	
Security Advisory SA55314 - Oracle Solaris Perl Multiple Vulnerabilities - Secunia	SECUNIA	<a href="https://secunia.com">secunia.com</a>	
Repository / Oval Repository	OVAL	<a href="https://oval.cisecurity.org">oval.cisecurity.org</a>	
'[USN-72-1] Perl vulnerabilities' - MARC	BUGTRAQ	<a href="https://marc.info">marc.info</a>	
2005-0003	TRUSTIX	<a href="https://www.trustix.org">www.trustix.org</a>	Patch, '...
<a href="http://www.digitalmunition.com/DMA[2005-0131b].txt">www.digitalmunition.com/DMA[2005-0131b].txt</a>	MISC	<a href="http://www.digitalmunition.com">www.digitalmunition.com</a>	Broken
Perl SuidPerl Multiple Local Vulnerabilities	BID	<a href="https://www.securityfocus.com">www.securityfocus.com</a>	Patch, '...
IBM X-Force Exchange	XF	<a href="https://exchange.xforce.ibmcloud.com">exchange.xforce.ibmcloud.com</a>	
'[Full-Disclosure] DMA[2005-0131b] - 'Setuid Perl PERLIO_DEBUG' - MARC	FULLDISC	<a href="https://marc.info">marc.info</a>	
Gentoo Linux Documentation -- Perl: Vulnerabilities in perl-suid wrapper	GENTOO	<a href="https://www.gentoo.org">www.gentoo.org</a>	Exploit, '...
404 Not Found		<a href="http://www.digitalmunition.com">www.digitalmunition.com</a>	
<a href="https://rhn.redhat.com">rhn.redhat.com</a>   Red Hat Support	REDHAT	<a href="https://www.redhat.com">www.redhat.com</a>	Patch, '...
<a href="https://rhn.redhat.com">rhn.redhat.com</a>   Red Hat Support	REDHAT	<a href="https://www.redhat.com">www.redhat.com</a>	Patch, '...
Home - Conectiva	CONNECTIVA	<a href="https://distro.conectiva.com.br">distro.conectiva.com.br</a>	
404 Not Found	FEDORA	<a href="https://fedoraneews.org">fedoraneews.org</a>	
Advisories - Mandriva	MANDRAKE	<a href="https://www.mandriva.com">www.mandriva.com</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonic
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonic

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](#)**