



# CVE-2004-0884

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

## Summary

<b>CVE</b>	CVE-2004-0884
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2005-01-27 05:00:00 UTC
<b>Updated</b>	2017-10-11 01:29:00 UTC
<b>Description</b>	The (1) libsas1 and (2) libsas2 libraries in Cyrus-SASL 2.1.18 and earlier trust the SASL_PATH environment variable to find

## 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>	10.0	All	All	All
Operating System	<a href="#">Conectiva</a>	<a href="#">Linux</a>	9.0	All	All	All
Operating System	<a href="#">Conectiva</a>	<a href="#">Linux</a>	10.0	All	All	All
Operating System	<a href="#">Conectiva</a>	<a href="#">Linux</a>	9.0	All	All	All
Application	<a href="#">Cyrus</a>	<a href="#">Sasl</a>	1.5.24	All	All	All
Application	<a href="#">Cyrus</a>	<a href="#">Sasl</a>	1.5.27	All	All	All
Application	<a href="#">Cyrus</a>	<a href="#">Sasl</a>	1.5.28	All	All	All
Application	<a href="#">Cyrus</a>	<a href="#">Sasl</a>	2.1.10	All	All	All
Application	<a href="#">Cyrus</a>	<a href="#">Sasl</a>	2.1.11	All	All	All
Application	<a href="#">Cyrus</a>	<a href="#">Sasl</a>	2.1.12	All	All	All
Application	<a href="#">Cyrus</a>	<a href="#">Sasl</a>	2.1.13	All	All	All
Application	<a href="#">Cyrus</a>	<a href="#">Sasl</a>	2.1.14	All	All	All
Application	<a href="#">Cyrus</a>	<a href="#">Sasl</a>	2.1.15	All	All	All
Application	<a href="#">Cyrus</a>	<a href="#">Sasl</a>	2.1.16	All	All	All
Application	<a href="#">Cyrus</a>	<a href="#">Sasl</a>	2.1.17	All	All	All
Application	<a href="#">Cyrus</a>	<a href="#">Sasl</a>	2.1.18	All	All	All
Application	<a href="#">Cyrus</a>	<a href="#">Sasl</a>	2.1.18_r1	All	All	All

Application	<a href="#">Cyrus</a>	<a href="#">Sasl</a>	2.1.9	All	All	All
Application	<a href="#">Cyrus</a>	<a href="#">Sasl</a>	1.5.24	All	All	All
Application	<a href="#">Cyrus</a>	<a href="#">Sasl</a>	1.5.27	All	All	All
Application	<a href="#">Cyrus</a>	<a href="#">Sasl</a>	1.5.28	All	All	All
Application	<a href="#">Cyrus</a>	<a href="#">Sasl</a>	2.1.10	All	All	All
Application	<a href="#">Cyrus</a>	<a href="#">Sasl</a>	2.1.11	All	All	All
Application	<a href="#">Cyrus</a>	<a href="#">Sasl</a>	2.1.12	All	All	All
Application	<a href="#">Cyrus</a>	<a href="#">Sasl</a>	2.1.13	All	All	All
Application	<a href="#">Cyrus</a>	<a href="#">Sasl</a>	2.1.14	All	All	All
Application	<a href="#">Cyrus</a>	<a href="#">Sasl</a>	2.1.15	All	All	All
Application	<a href="#">Cyrus</a>	<a href="#">Sasl</a>	2.1.16	All	All	All
Application	<a href="#">Cyrus</a>	<a href="#">Sasl</a>	2.1.17	All	All	All
Application	<a href="#">Cyrus</a>	<a href="#">Sasl</a>	2.1.18	All	All	All
Application	<a href="#">Cyrus</a>	<a href="#">Sasl</a>	2.1.18_r1	All	All	All
Application	<a href="#">Cyrus</a>	<a href="#">Sasl</a>	2.1.9	All	All	All

## References

Reference	Source	Link
redhat.com   Red Hat Support	REDHAT	<a href="http://rhn.redhat.com">rhn.redhat.com</a>
APPLE-SA-2005-03-21 Security Update 2005-003	APPLE	<a href="http://lists.apple.com">lists.apple.com</a>
P-003: Updated Cyrus-SASL Packages Fix Security Flaw	CIAC	<a href="http://www.ciac.org">www.ciac.org</a>
Repository / Oval Repository	OVAL	<a href="http://oval.cisecurity.org">oval.cisecurity.org</a>
Debian -- Security Information -- DSA-563-3 cyrus-sasl	DEBIAN	<a href="http://www.debian.org">www.debian.org</a>
IBM X-Force Exchange	XF	<a href="http://exchange.xforce.ibmcloud.com">exchange.xforce.ibmcloud.com</a>
Cyrus SASL Multiple Remote And Local Vulnerabilities	BID	<a href="http://www.securityfocus.com">www.securityfocus.com</a>
'[OpenPKG-SA-2005.004] OpenPKG Security Advisory (sasl)' - MARC	BUGTRAQ	<a href="http://marc.info">marc.info</a>
FLSA:2137	FEDORA	<a href="http://bugzilla.fedora.us">bugzilla.fedora.us</a>
134657 – CAN-2004-0884 privilege escalation	CONFIRM	<a href="http://bugzilla.redhat.com">bugzilla.redhat.com</a>
2004-0053	TRUSTIX	<a href="http://www.trustix.net">www.trustix.net</a>
Gentoo Linux Documentation -- Cyrus-SASL: Buffer overflow and SASL_PATH vulnerabilities	GENTOO	<a href="http://www.gentoo.org">www.gentoo.org</a>
Advisories - Mandriva	MANDRAKE	<a href="http://www.mandriva.com">www.mandriva.com</a>
Debian -- Security Information -- DSA-568-1 cyrus-sasl-mit	DEBIAN	<a href="http://www.debian.org">www.debian.org</a>
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>

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](#)**