



CVE-2002-2253

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

Summary

CVE	CVE-2002-2253
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2002-12-31 05:00:00 UTC
Updated	2017-07-29 01:29:00 UTC
Description	Multiple buffer overflows in Cyrus Sieve / libSieve 2.1.2 and earlier allow remote attackers to execute arbitrary code via (1) :

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cyrus	Libsieve	All	All	All	All

References

Reference	Source	Link	Ta
libSieve Error Message Buffer Overrun Vulnerability	BID	www.securityfocus.com	
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com	
libSieve IMAP Flag Buffer Overrun Vulnerability	BID	www.securityfocus.com	
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com	
Neohapsis Archives - Bugtraq - Cyrus Sieve / libSieve buffer overflow - From tss_at_iki.fi	BUGTRAQ	archives.neohapsis.com	Ex
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com	
libSieve Header Name Buffer Overrun Vulnerability	BID	www.securityfocus.com	
CVE Program record	CVE.ORG	www.cve.org	ca
NVD vulnerability detail	NVD	nvd.nist.gov	ca

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](#)