



# CVE-2004-1011

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

## Summary

<b>CVE</b>	CVE-2004-1011
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2005-01-10 05:00:00 UTC
<b>Updated</b>	2017-07-11 01:30:00 UTC
<b>Description</b>	Stack-based buffer overflow in Cyrus IMAP Server 2.2.4 through 2.2.8, with the imapmagicplus option enabled, allows remote

## Risk And Classification

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

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Carnegie Mellon University	Cyrus Imap Server	2.1.10	All	All	All
Application	Carnegie Mellon University	Cyrus Imap Server	2.1.16	All	All	All
Application	Carnegie Mellon University	Cyrus Imap Server	2.1.7	All	All	All
Application	Carnegie Mellon University	Cyrus Imap Server	2.1.9	All	All	All
Application	Carnegie Mellon University	Cyrus Imap Server	2.2.0_alpha	All	All	All
Application	Carnegie Mellon University	Cyrus Imap Server	2.2.1_beta	All	All	All
Application	Carnegie Mellon University	Cyrus Imap Server	2.2.2_beta	All	All	All
Application	Carnegie Mellon University	Cyrus Imap Server	2.2.3	All	All	All
Application	Carnegie Mellon University	Cyrus Imap Server	2.2.4	All	All	All
Application	Carnegie Mellon University	Cyrus Imap Server	2.2.5	All	All	All
Application	Carnegie Mellon University	Cyrus Imap Server	2.2.6	All	All	All
Application	Carnegie Mellon University	Cyrus Imap Server	2.2.7	All	All	All
Application	Carnegie Mellon University	Cyrus Imap Server	2.2.8	All	All	All
Application	Carnegie Mellon University	Cyrus Imap Server	2.1.10	All	All	All
Application	Carnegie Mellon University	Cyrus Imap Server	2.1.16	All	All	All
Application	Carnegie Mellon University	Cyrus Imap Server	2.1.7	All	All	All
Application	Carnegie Mellon University	Cyrus Imap Server	2.1.9	All	All	All

Application	<a href="#">Carnegie Mellon University</a>	<a href="#">Cyrus Imap Server</a>	2.2.0_alpha	All	All	All
Application	<a href="#">Carnegie Mellon University</a>	<a href="#">Cyrus Imap Server</a>	2.2.1_beta	All	All	All
Application	<a href="#">Carnegie Mellon University</a>	<a href="#">Cyrus Imap Server</a>	2.2.2_beta	All	All	All
Application	<a href="#">Carnegie Mellon University</a>	<a href="#">Cyrus Imap Server</a>	2.2.3	All	All	All
Application	<a href="#">Carnegie Mellon University</a>	<a href="#">Cyrus Imap Server</a>	2.2.4	All	All	All
Application	<a href="#">Carnegie Mellon University</a>	<a href="#">Cyrus Imap Server</a>	2.2.5	All	All	All
Application	<a href="#">Carnegie Mellon University</a>	<a href="#">Cyrus Imap Server</a>	2.2.6	All	All	All
Application	<a href="#">Carnegie Mellon University</a>	<a href="#">Cyrus Imap Server</a>	2.2.7	All	All	All
Application	<a href="#">Carnegie Mellon University</a>	<a href="#">Cyrus Imap Server</a>	2.2.8	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
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="#">Openpkg</a>	<a href="#">Openpkg</a>	current	All	All	All
Application	<a href="#">Openpkg</a>	<a href="#">Openpkg</a>	current	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Fedora Core</a>	core_2.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Fedora Core</a>	core_3.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Fedora Core</a>	core_2.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Fedora Core</a>	core_3.0	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>	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
IBM X-Force Exchange	XF	<a href="https://exchange.xforce.ibmcloud.com">exchange.xforce.ibmcloud.com</a>	
Secunia - Advisories - Cyrus IMAP Server Multiple Vulnerabilities	SECUNIA	<a href="https://secunia.com">secunia.com</a>	
Gentoo Linux Documentation -- Cyrus IMAP Server: Multiple remote vulnerabilities	GENTOO	<a href="https://security.gentoo.org">security.gentoo.org</a>	

'Advisory 15/2004: Cyrus IMAP Server multiple remote vulnerabilities' - MARC	BUG I HAQ	<a href="http://marc.info">marc.info</a>	
Advisories - Mandriva	MANDRAKE	<a href="http://www.mandriva.com">www.mandriva.com</a>	
[cyrus-announce] 20041122 Cyrus IMAPd 2.2.9 Released	MLIST	<a href="mailto:asg.web.cmu.edu">asg.web.cmu.edu</a>	
e-matters : SECURITY	MISC	<a href="http://security.e-matters.de">security.e-matters.de</a>	
Changes to the Cyrus IMAP Server	CONFIRM	<a href="mailto:asg.web.cmu.edu">asg.web.cmu.edu</a>	
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonic
NVD vulnerability detail	NVD	<a href="http://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](http://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](http://The MITRE Corporation) and the authoritative source of CVE content is [MITRE's CVE web site](http://MITRE's CVE web site). This site includes MITRE data granted under the following [license](http://license).

**CVE.report and Source URL Uptime Status [status.cve.report](http://status.cve.report)**