



CVE-2005-2933

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

Summary

CVE	CVE-2005-2933
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2005-10-13 22:02:00 UTC
Updated	2018-10-19 15:34:00 UTC
Description	Buffer overflow in the mail_valid_net_parse_work function in mail.c for Washington's IMAP Server (UW-IMAP) before imap-

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)


Type	Vendor	Product	Version	Update	Edition	Language
Application	University Of Washington	Uw-imap	2004	All	All	All
Application	University Of Washington	Uw-imap	2004a	All	All	All
Application	University Of Washington	Uw-imap	2004b	All	All	All
Application	University Of Washington	Uw-imap	2004c	All	All	All
Application	University Of Washington	Uw-imap	2004d	All	All	All
Application	University Of Washington	Uw-imap	2004e	All	All	All
Application	University Of Washington	Uw-imap	2004	All	All	All
Application	University Of Washington	Uw-imap	2004a	All	All	All
Application	University Of Washington	Uw-imap	2004b	All	All	All
Application	University Of Washington	Uw-imap	2004c	All	All	All
Application	University Of Washington	Uw-imap	2004d	All	All	All
Application	University Of Washington	Uw-imap	2004e	All	All	All
Application	University Of Washington	Uw-imap	All	All	All	All

References

Reference

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

Debian -- Security Information -- DSA-861-1 uw-imap
Secunia - Advisories - Red Hat update for libc-client
Avaya Products PHP Multiple Vulnerabilities - Advisories - Secunia
Secunia - Advisories - UW-imapd Mailbox Name Parsing Buffer Overflow Vulnerability
Accenture Let there be change
Advisories - Mandriva Linux
Secunia - Advisories - Gentoo update for uw-imap
SecurityTracker.com Archives - UW-IMAP Buffer Overflow in Processing Mailbox Name Lets Remote Authenticated Users Execute Arbitrary C
The Slackware Linux Project: Slackware Security Advisories
rhn.redhat.com Red Hat Support
University Of Washington IMAP Mailbox Name Buffer Overflow Vulnerability
rhn.redhat.com Red Hat Support
Security Announcement
UW-IMAP Netmailbox Name Parsing Buffer Overflow Vulnerability - CXSecurity.com
Repository / Oval Repository
UW IMAP software--IMAP Information Center
Secunia - Advisories - SGI Advanced Linux Environment Multiple Updates
20051201-01-U
Red Hat Stronghold updates for uw-imap and PHP - Advisories - Secunia
Secunia - Advisories - Red Hat update for imap
Secunia - Advisories - Slackware update for imapd
rhn.redhat.com Red Hat Support
SecurityFocus
rhn.redhat.com Red Hat Support
Secunia - Advisories - Fedora update for libc-client
20060501-01-U
rhn.redhat.com Red Hat Support
Gentoo Linux Documentation -- uw-imap: Remote buffer overflow
ASA-2006-129 (RHSA-2006-0276)
Secunia - Advisories - Debian update for uw-imap
Secunia - Advisories - Avaya Products PHP Multiple Vulnerabilities
Advisories - Mandriva
Neohapsis Archives - Full Disclosure List - #0081 - [Full-disclosure] iDEFENSE Security Advisory 10.04.05: UW-IMAP Netmailbox Name Pars
ASA-2006-160 (RHSA-2006-0501)
Secunia - Advisories - SUSE Updates for Multiple Packages

Secunia - Advisories - Mandriva update tor imap
Red Hat update for php - Advisories - Secunia
Secunia - Advisories - Mandriva update for php-imap
SecurityFocus
Secunia - Advisories - SGI Advanced Linux Environment Multiple Updates
US-CERT Vulnerability Note VU#933601
IBM X-Force Exchange
Red Hat update for php - Advisories - Secunia
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.
There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status status.cve.report