



CVE-2004-2501

Published on: 12/31/2004 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:14 PM UTC

CVE-2004-2501

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Mailenable Enterprise](#) from [Mailenable](#) contain the following vulnerability:

Buffer overflow in the IMAP service of MailEnable Professional Edition 1.52 and Enterprise Edition 1.01 allows remote attackers to execute arbitrary code via (1) a long command string or (2) a long string to the MEIMAP service and then terminating the connection.

CVE-2004-2501 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **7.5 - HIGH**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

PARTIAL

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

IBM X-Force Exchange

[exchange.xforce.ibmcloud.com
text/html](https://exchange.xforce.ibmcloud.com/text/html)

[XF mailenable-imap-code-execution\(18286\)](#)

:::Hat-Squad Security Group:::

[Exploit](#)
[Patch](#)
[Vendor Advisory](#)
www.hat-squad.com
[text/x-c](#)

[MISC www.hat-squad.com/en/000102.html](#)

IBM X-Force Exchange

[exchange.xforce.ibmcloud.com
text/html](https://exchange.xforce.ibmcloud.com/text/html)

[XF mailenable-imap-bo\(18285\)](#)

No Description Provided

www.osvdb.org

[OSVDB 12135](#)

Inactive Link **Not Archived**

MailEnable IMAP Service Multiple Remote Pre-Authentication Buffer

[Exploit](#)

[BID 11755](#)

Overflow Vulnerabilities	Patch cve.report (archive) text/html	
Secunia - Advisories - MailEnable IMAP Service Buffer Overflow Vulnerabilities	Patch Vendor Advisory web.archive.org text/html	 SECUNIA 13318
No Description Provided	www.osvdb.org Inactive Link Not Archived	 OSVDB 12136
SecurityTracker.com Archives - MailEnable Stack Overflow and Pointer Overwrite in IMAP Service Lets Remote Users Execute Arbitrary Code	Exploit Patch Vendor Advisory securitytracker.com text/html	 SECTRAK 1012327
Neohapsis Archives - Bugtraq - #0349 - Remote buffer overflow in MailEnable IMAP service [Hat-Squad Advisory]	Exploit Patch Vendor Advisory archives.neohapsis.com text/x-c Inactive Link Not Archived	 BUGTRAQ 20041125 Remote buffer overflow in MailEnable IMAP service [Hat-Squad Advisory]
By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.		

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Application	Mailenable	Mailenable Enterprise	1.01	All	All	All
Application	Mailenable	Mailenable Enterprise	1.01	All	All	All
Application	Mailenable	Mailenable Professional	1.52	All	All	All
Application	Mailenable	Mailenable Professional	1.52	All	All	All
cpe:2.3:a:mailenable:mailenable_enterprise:1.01:*****:*						
cpe:2.3:a:mailenable:mailenable_enterprise:1.01:*****:*						
cpe:2.3:a:mailenable:mailenable_professional:1.52:*****:*						
cpe:2.3:a:mailenable:mailenable_professional:1.52:*****:*						

No vendor comments have been submitted for this CVE

© [CVE.report](#) 2023   |

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](#)