



CVE-2005-4402

Published on: 12/20/2005 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:21 PM UTC

CVE-2005-4402

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

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

Buffer overflow in MailEnable Professional 1.71 and earlier, and Enterprise 1.1 and earlier, allows remote authenticated users to execute arbitrary code via a long IMAP EXAMINE command.

CVE-2005-4402 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **6.5 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

SINGLE

Confidentiality
Impact

PARTIAL

Integrity
Impact

PARTIAL

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

'[Full-disclosure] Remote Buffer Overflow in Mailenable Enterprise' - MARC

[marc.info](#)
[text/html](#)

[FULLDISC 20051219 Remote Buffer Overflow in Mailenable Enterprise](#)

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

[www.vupen.com](#)
[text/html](#)

[VUPEN ADV-2005-2988](#)

SecurityTracker.com Archives - MailEnable Buffer Overflow in IMAP EXAMINE Command Lets Remote Authenticated Users Execute Arbitrary Code

[securitytracker.com](#)
[text/html](#)

[SECTrack 1015378](#)

MailEnable™ - Hot Fixes Download Page

[Patch](#)
[www.mailenable.com](#)
[text/html](#)

[MISC](#)
[www.mailenable.com/hotfix/](#)

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,

are more appropriate for your purposes. CVE.report does not necessarily endorse the views expressed, or content that are made available on these sites. CVE.report 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	All	All	All	All
Application	Mailenable	Mailenable Professional	All	All	All	All
cpe:2.3:a:mailenable:mailenable_enterprise:*****:.*						
cpe:2.3:a:mailenable:mailenable_professional:*****:.*						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)