



CVE-2006-6290

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2006-6290
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-12-05 11:28:00 UTC
Updated	2026-04-23 00:35:47 UTC
Description	Multiple stack-based buffer overflows in the IMAP module (MEIMAPS.EXE) in MailEnable Professional 1.6 through 1.82 an

Risk And Classification

Primary CVSS: v2.0 6.5 from nvd@nist.gov

AV:N/AC:L/Au:S/C:P/I:P/A:P

Problem Types: NVD-CWE-Other | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

Single

Confidentiality

Partial

Integrity

Partial

Availability

Partial

AV:N/AC:L/Au:S/C:P/I:P/A:P

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mailenable	Mailenable Enterprise	1.1	All	All	All

Application	Mailenable	Mailenable Enterprise	2.17	All	All	All
Application	Mailenable	Mailenable Enterprise	2.18	All	All	All
Application	Mailenable	Mailenable Enterprise	2.19	All	All	All
Application	Mailenable	Mailenable Enterprise	2.2	All	All	All
Application	Mailenable	Mailenable Enterprise	2.21	All	All	All
Application	Mailenable	Mailenable Enterprise	2.22	All	All	All
Application	Mailenable	Mailenable Enterprise	2.23	All	All	All
Application	Mailenable	Mailenable Enterprise	2.24	All	All	All
Application	Mailenable	Mailenable Enterprise	2.25	All	All	All
Application	Mailenable	Mailenable Enterprise	2.26	All	All	All
Application	Mailenable	Mailenable Enterprise	2.27	All	All	All
Application	Mailenable	Mailenable Enterprise	2.28	All	All	All
Application	Mailenable	Mailenable Enterprise	2.29	All	All	All
Application	Mailenable	Mailenable Enterprise	2.30	All	All	All
Application	Mailenable	Mailenable Enterprise	2.31	All	All	All
Application	Mailenable	Mailenable Enterprise	2.32	All	All	All
Application	Mailenable	Mailenable Enterprise	2.33	All	All	All
Application	Mailenable	Mailenable Professional	1.6	All	All	All
Application	Mailenable	Mailenable Professional	1.82	All	All	All
Application	Mailenable	Mailenable Professional	2.0	All	All	All
Application	Mailenable	Mailenable Professional	2.33	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference
IBM X-Force Exchange
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
MailEnable™ - Hot Fixes Download Page
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
MailEnable IMAP Service Two Vulnerabilities - Secunia Research - Secunia
MailEnable IMAP Service Multiple Buffer Overflow Vulnerabilities
SecurityFocus
SecurityTracker.com Archives - MailEnable IMAP Bugs Let Remote Authenticated Users Deny Service and Potentially Execute Arbitrary Code

MailEnable IMAP Service Two Vulnerabilities - Advisories - Secunia

SecurityTracker.com Archives - MailEnable Buffer Overflow in IMAP Service May Let Remote Users Execute Arbitrary Code

MailEnable IMAP Service Buffer Overflow Vulnerability - 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](#) 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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)