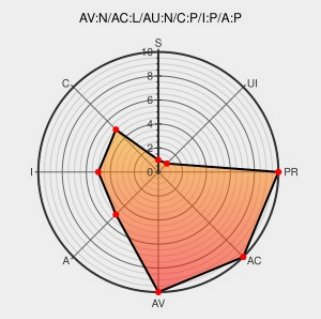
CVE-2004-2501

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 cve@mitre.org to track the vulnerability

CVSS2 Score: 7.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
IBM X-Force Exchange	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	XF mailenable-imap-bo(18285)
No Description Provided	www.osvdb.org, Inactive Link, Not Archived	OSVDB 12135
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	SECTRACK 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]

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

← Previous ID

Next ID→

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