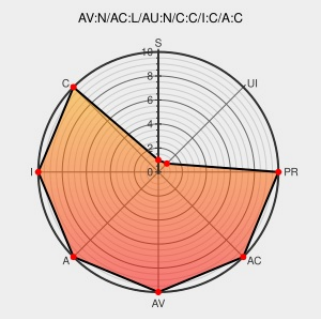
CVE-2006-1255

Published on: 03/18/2006 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:00 PM UTC

CVE-2006-1255

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Mercur Messaging from Mercur contain the following vulnerability:

Stack-based buffer overflow in the IMAP service in Mercur Messaging 5.0 SP3 and earlier allows remote attackers to cause a denial of service (application crash) and possibly execute arbitrary code via a long string to the (1) LOGIN or (2) SELECT command, a different set of attack vectors and possibly a different vulnerability than CVE-2003-1177.

CVE-2006-1255 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 10 - HIGH

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

CVE References

Description	Tags	Link
Full Disclosure: Re: Mercur IMAPD 5.0 SP3 DoS Exploit or more?	seclists.org text/html	FULLDISC 20060316 Re: Mercur IMAPD 5.0 SP3 DoS Exploit or more?
MERCUR Messaging 2005 IMAP Remote Buffer Overflow Vulnerability	cve.report (archive) text/html	BID 17138
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com text/html	VUPEN ADV-2006-0977
No Description Provided	www.osvdb.org Inactive Link Not Archived	OSVDB 23950
Full Disclosure: Mercur IMAPD 5.0 SP3 DoS Exploit or	seclists.org	FULLDISC 20060316 Mercur IMAPD 5.0

more?	text/html	SP3 DoS Exploit or more?
Mercur Messaging IMAP Service Multiple Buffer Overflows - Advisories - Secunia	Exploit Vendor Advisory web.archive.org text/html	SECUNIA 19267
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF mercur-imap-bo(25290)

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mercur	Mercur Messaging	All	All	All	All

cpe:2.3:a:mercur:mercur_messaging:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→