



CVE-2004-2447

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

Last Modified on: 03/23/2021 11:28:13 PM UTC

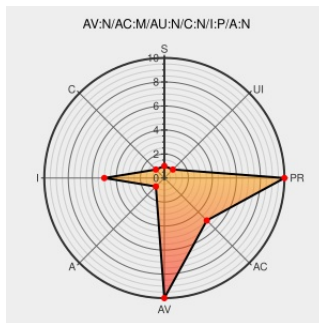
CVE-2004-2447

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [1st Class Mail Server](#) from [1st Class Internet Solutions](#) contain the following vulnerability:

Cross-site scripting (XSS) vulnerability in 1st Class Mail Server 4.01 allows remote attackers to inject arbitrary web script or HTML via the Mailbox parameter to (1) viewmail.tagz, (2) the index script under /user/, (3) members.tagz, (4) general.tagz, (5) advanced.tagz, or (6) list.tagz.

CVE-2004-2447 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **4.3 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
No Description Provided	Exploit www.osvdb.org	OSVDB 5017
	Inactive Link Not Archived	
No Description Provided	Exploit www.osvdb.org	OSVDB 5015
	Inactive Link Not Archived	
1st Class Internet Solutions 1st Class Mail Server Multiple Input Validation Vulnerabilities	Exploit cve.report (archive) text/html	BID 10089
IBM X-Force Exchange	exchange.xforce.ibmcloud.com	XF

	text/html	1stclass-multiple-xss(15815)
Secunia - Advisories - 1st Class Mail Server Directory Traversal and Cross Site Scripting	Exploit Vendor Advisory web.archive.org text/html	 SECUNIA 11330
No Description Provided	Exploit www.osvdb.org Inactive Link Not Archived	 OSVDB 5016
No Description Provided	Exploit www.osvdb.org Inactive Link Not Archived	 OSVDB 5014
SecurityTracker.com Archives - 1st Class Mail Server Input Validation Holes Disclose Files to Remote Users and Permit Cross-Site Scripting Attacks	Exploit Vendor Advisory securitytracker.com text/html	 SECTRACK 1009705
No Description Provided	Exploit www.osvdb.org Inactive Link Not Archived	 OSVDB 5013
No Description Provided	Exploit www.osvdb.org Inactive Link Not Archived	 OSVDB 5012

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	1st Class Internet Solutions	1st Class Mail Server	4.01	All	All	All
Application	1st Class Internet Solutions	1st Class Mail Server	4.01	All	All	All
cpe:2.3:a:1st_class_internet_solutions:1st_class_mail_server:4.01:*****:*						
cpe:2.3:a:1st_class_internet_solutions:1st_class_mail_server:4.01:*****:*						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

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](#)