



CVE-2005-1254

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2005-1254
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2005-05-25 04:00:00 UTC
Updated	2008-11-15 05:46:00 UTC
Description	Stack-based buffer overflow in the IMAP server for Ipswitch IMail 8.12 and 8.13, and other versions before IMail Server 8.2

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ipswitch	Imail	8.12	All	All	All
Application	Ipswitch	Imail	8.13	All	All	All
Application	Ipswitch	Imail	8.12	All	All	All
Application	Ipswitch	Imail	8.13	All	All	All
Application	Ipswitch	Imail	All	All	All	All

References

Reference	Source	Link
Accenture Let there be change	IDEFENSE	www.iddefense
Ipswitch, Inc. - IMail Server Patches & Upgrades	CONFIRM	www.ipswitch.
Ipswitch IMail Server Multiple Vulnerabilities	BID	www.securityf
SecurityTracker.com Archives - IPswitch IMail Bugs Let Remote Users View Files and Execute Arbitrary Code	SECTRACK	securitytracke
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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](#).

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