



# CVE-2007-1578

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2007-1578
<b>State</b>	PUBLISHED
<b>Assigner</b>	mitre
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2007-03-21 23:19:00 UTC
<b>Updated</b>	2026-04-23 00:35:47 UTC
<b>Description</b>	Multiple integer signedness errors in the NTLM implementation in Atrium MERCUR IMAPD (mcrimap4.exe) 5.00.14, with S

## Risk And Classification

**Primary CVSS:** v2.0 10 from nvd@nist.gov

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

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

## CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

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

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Atrium Software	Mercur Imapd	5.00.14	sp4	All	All

## Vendor Declared Affected Products

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

## References

Reference	Source
Mercur IMAPD 5.00.14 (Windows x86) - Remote Denial of Service - Windows_x86 dos Exploit	af854a3a-2127-42
Webmail- OVH	af854a3a-2127-42
www.osvdb.org/33545	af854a3a-2127-42
MERCUR Mailserver NTLM IMAP Command Integer Signedness Bug Permits Remote Code Execution - SecurityTracker	af854a3a-2127-42
Mercur Messaging IMAP NTLM Authentication Processing Vulnerabilities - Advisories - Secunia	af854a3a-2127-42
IBM X-Force Exchange	af854a3a-2127-42
Atrium Mercur IMAPD NTLM Buffer Overflow Vulnerability	af854a3a-2127-42
www.digit-labs.org/files/exploits/mercur-v1.pl	af854a3a-2127-42
NEOHAPSIS - Peace of Mind Through Integrity and Insight	af854a3a-2127-42
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

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](#)