



# CVE-2005-3901

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

|                        |  |
|------------------------|--|
| <b>CVE</b>             | CVE-2005-3901  |
| <b>State</b>           | PUBLIC   |
| <b>Assigner</b>        | cve@mitre.org  |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback   |
| <b>Published</b>       | 2005-11-29 22:03:00 UTC  |
| <b>Updated</b>         | 2008-09-05 20:55:00 UTC  |
| <b>Description</b>     | Macromedia Flash Communication Server MX 1.0 and 1.5 does not sufficiently validate certain RTMP data, which allows at |

## Risk And Classification

**Problem Types:** NVD-CWE-Other

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor     | Product                    | Version | Update | Edition | Language |
|-------------|------------|----------------------------|---------|--------|---------|----------|
| Application | Macromedia | Flash Communication Server | 1.0     | All    | All     | All      |
| Application | Macromedia | Flash Communication Server | 1.5     | All    | All     | All      |
| Application | Macromedia | Flash Communication Server | 1.0     | All    | All     | All      |
| Application | Macromedia | Flash Communication Server | 1.5     | All    | All     | All      |

## References

| Reference   | Source |
|---|--------|
| Macromedia - MPSB05-09 : Security Patch for Insufficient Validation in Flash Communication Server                       | CONF   |
| Macromedia Flash Communication Server MX RTMP Data Validation Vulnerability   | BID    |
| SecurityTracker.com Archives - Macromedia Flash Communication Server RTMP Processing Bug Lets Remote Users Deny Service | SECTF  |
| Secunia - Advisories - Macromedia Flash Communication Server MX Denial of Service                                       | SECUN  |
| 20869   | OSVDB  |
| CVE Program record  | CVE.O  |
| 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](#).

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