



# CVE-2004-0433

- MITRE
- NVD
- CVE.ORG
- JSON API
- Print: PDF

## Summary

|                 |                                                                                                                               |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------|
| CVE             | CVE-2004-0433                                                                                                                 |
| State           | PUBLISHED                                                                                                                     |
| Assigner        | mitre                                                                                                                         |
| Source Priority | CVE Program / NVD first with legacy fallback                                                                                  |
| Published       | 2004-08-18 04:00:00 UTC                                                                                                       |
| Updated         | 2025-04-03 01:03:51 UTC                                                                                                       |
| Description     | Multiple buffer overflows in the Real-Time Streaming Protocol (RTSP) client for (1) MPlayer before 1.0pre4 and (2) xine lib ( |

## 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 | Mplayer | Mplayer | 1.0_pre3try2 | All    | All     | All      |

|             |                      |                          |          |     |     |     |
|-------------|----------------------|--------------------------|----------|-----|-----|-----|
| Application | <a href="#">Xine</a> | <a href="#">Xine-lib</a> | 1_beta1  | All | All | All |
| Application | <a href="#">Xine</a> | <a href="#">Xine-lib</a> | 1_beta10 | All | All | All |
| Application | <a href="#">Xine</a> | <a href="#">Xine-lib</a> | 1_beta11 | All | All | All |
| Application | <a href="#">Xine</a> | <a href="#">Xine-lib</a> | 1_beta2  | All | All | All |
| Application | <a href="#">Xine</a> | <a href="#">Xine-lib</a> | 1_beta3  | All | All | All |
| Application | <a href="#">Xine</a> | <a href="#">Xine-lib</a> | 1_beta4  | All | All | All |
| Application | <a href="#">Xine</a> | <a href="#">Xine-lib</a> | 1_beta5  | All | All | All |
| Application | <a href="#">Xine</a> | <a href="#">Xine-lib</a> | 1_beta6  | All | All | All |
| Application | <a href="#">Xine</a> | <a href="#">Xine-lib</a> | 1_beta7  | All | All | All |
| Application | <a href="#">Xine</a> | <a href="#">Xine-lib</a> | 1_beta8  | All | All | All |
| Application | <a href="#">Xine</a> | <a href="#">Xine-lib</a> | 1_beta9  | All | All | All |
| Application | <a href="#">Xine</a> | <a href="#">Xine-lib</a> | 1_rc2    | All | All | All |
| Application | <a href="#">Xine</a> | <a href="#">Xine-lib</a> | 1_rc3a   | All | All | All |
| Application | <a href="#">Xine</a> | <a href="#">Xine-lib</a> | 1_rc3b   | All | All | All |
| Application | <a href="#">Xine</a> | <a href="#">Xine-lib</a> | 1_rc3c   | All | All | All |

| Vendor Declared Affected Products |        |         |              |               |
|-----------------------------------|--------|---------|--------------|---------------|
| Source                            | Vendor | Product | Version      | Platforms     |
| CNA                               | Na     | N/a     | affected n/a | Not specified |

| References                                                                               |                                      |                      |
|------------------------------------------------------------------------------------------|--------------------------------------|----------------------|
| Reference                                                                                | Source                               | Link                 |
| IBM X-Force Exchange                                                                     | af854a3a-2127-422b-91ae-364da2661108 | <a href="#">exch</a> |
| xine - A Free Video Player - Home                                                        | af854a3a-2127-422b-91ae-364da2661108 | <a href="#">www</a>  |
| Gentoo Linux Documentation -- MPlayer, xine-lib: vulnerabilities in RTSP stream handling | af854a3a-2127-422b-91ae-364da2661108 | <a href="#">secu</a> |
| CVE Program record                                                                       | CVE.ORG                              | <a href="#">www</a>  |
| NVD vulnerability detail                                                                 | NVD                                  | <a href="#">nvd.</a> |

|                                                                      |
|----------------------------------------------------------------------|
| No vendor comments have been submitted for this CVE.                 |
| There are currently no legacy QID mappings associated with this CVE. |

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](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)