



# CVE-2004-2433

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

## Summary

|                 |                                                                                                                              |
|-----------------|------------------------------------------------------------------------------------------------------------------------------|
| CVE             | CVE-2004-2433                                                                                                                |
| State           | PUBLISHED                                                                                                                    |
| Assigner        | mitre                                                                                                                        |
| Source Priority | CVE Program / NVD first with legacy fallback                                                                                 |
| Published       | 2004-12-31 05:00:00 UTC                                                                                                      |
| Updated         | 2025-04-03 01:03:51 UTC                                                                                                      |
| Description     | Buffer overflow in the IsValidFile function in the ADM ActiveX control for Altnet Download Manager 4.0.0.4 and earlier, as u |

## Risk And Classification

Primary CVSS: v2.0 7.5 from nvd@nist.gov

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

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

## CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

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

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor | Product                 | Version | Update | Edition | Language |
|-------------|--------|-------------------------|---------|--------|---------|----------|
| Application | Altnet | Altnet Download Manager | 4.0.0.4 | All    | All     | All      |

|             |                          |                                         |       |     |     |     |
|-------------|--------------------------|-----------------------------------------|-------|-----|-----|-----|
| Application | <a href="#">Altnet</a>   | <a href="#">Altnet Download Manager</a> | All   | All | All | All |
| Application | <a href="#">Grokster</a> | <a href="#">Grokster</a>                | 1.3   | All | All | All |
| Application | <a href="#">Grokster</a> | <a href="#">Grokster</a>                | 1.3.3 | All | All | All |
| Application | <a href="#">Grokster</a> | <a href="#">Grokster</a>                | 2.6   | All | All | All |
| Application | <a href="#">Kazaa</a>    | <a href="#">Kazaa Media Desktop</a>     | 1.3   | All | All | All |
| Application | <a href="#">Kazaa</a>    | <a href="#">Kazaa Media Desktop</a>     | 1.3.1 | All | All | All |
| Application | <a href="#">Kazaa</a>    | <a href="#">Kazaa Media Desktop</a>     | 1.3.2 | All | All | All |
| Application | <a href="#">Kazaa</a>    | <a href="#">Kazaa Media Desktop</a>     | 1.6.1 | All | All | All |
| Application | <a href="#">Kazaa</a>    | <a href="#">Kazaa Media Desktop</a>     | 2.0   | All | All | All |
| Application | <a href="#">Kazaa</a>    | <a href="#">Kazaa Media Desktop</a>     | 2.0.2 | All | All | All |
| Application | <a href="#">Kazaa</a>    | <a href="#">Kazaa Media Desktop</a>     | 2.6.4 | All | All | All |

| Vendor Declared Affected Products |                    |                     |              |               |
|-----------------------------------|--------------------|---------------------|--------------|---------------|
| Source                            | Vendor             | Product             | Version      | Platforms     |
| CNA                               | <a href="#">Na</a> | <a href="#">N/a</a> | affected n/a | Not specified |

| References                                                                                                                      |                       |
|---------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| Reference                                                                                                                       | Source                |
| Altnet ADM ActiveX Control Remote Buffer Overflow Vulnerability                                                                 | <a href="#">af854</a> |
| Secunia - Advisories - Grokster Altnet Download Manager Buffer Overflow Vulnerability                                           | <a href="#">af854</a> |
| IBM X-Force Exchange                                                                                                            | <a href="#">af854</a> |
| <a href="#">www.osvdb.org/9549</a>                                                                                              | <a href="#">af854</a> |
| Secunia - Advisories - Altnet Download Manager Buffer Overflow Vulnerability                                                    | <a href="#">af854</a> |
| SecurityTracker.com Archives - Altnet Download Manager Buffer Overflow in bstrFilepath Lets Remote Users Execute Arbitrary Code | <a href="#">af854</a> |
| CVE Program record                                                                                                              | <a href="#">CVE.c</a> |
| NVD vulnerability detail                                                                                                        | <a href="#">NVD</a>   |

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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)