



CVE-2005-0313

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

Summary

| | |
|------------------------|--|
| CVE | CVE-2005-0313 |
| State | PUBLISHED |
| Assigner | mitre |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2005-01-27 05:00:00 UTC |
| Updated | 2025-04-03 01:03:51 UTC |
| Description | Multiple directory traversal vulnerabilities in Magic Winmail Server 4.0 Build 1112 allow remote attackers to (1) upload arbit |

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

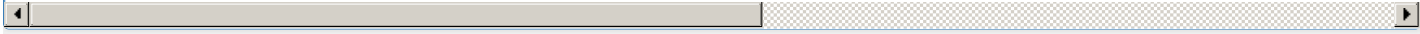
Partial

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 | Amax Information Technologies | Magic Winmail Server | 4.0 | All | All | All |

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

| References | |
|---|--|
| Reference | |
| Secunia - Advisories - Winmail Server Multiple Vulnerabilities | |
| '[SIG^2 G-TEC] Magic Winmail Server v4.0 Multiple Vulnerabilities' - MARC | |
| IBM X-Force Exchange | |
| IBM X-Force Exchange | |
| Magic Winmail Server Multiple Vulnerabilities | |
| SecurityTracker.com Archives - Magic Winmail Server Input Validation Holes in Webmail and IMAP Services Allow Directory Traversal Attacks | |
| CVE Program record | |
| NVD vulnerability detail | |
|  | |
| No vendor comments have been submitted for this CVE. | |
| There are currently no legacy QID mappings associated with this CVE. | |

© [CVE.report](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). 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