



CVE-2005-1393

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

Summary

| | |
|------------------------|---|
| CVE | CVE-2005-1393 |
| State | PUBLISHED |
| Assigner | mitre |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2005-05-03 04:00:00 UTC |
| Updated | 2025-04-03 01:03:51 UTC |
| Description | Multiple buffer overflows in ArcGIS for ESRI ArcInfo Workstation 9.0 allow local users to execute arbitrary code via long cor |

Risk And Classification

Primary CVSS: v2.0 4.6 from nvd@nist.gov

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

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

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

AV:L/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 | Esri | Arcinfo Workstation | 9.0 | All | All | All |

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

| References | |
|---|------------------------------|
| Reference | Source |
| Secunia - Advisories - ArcInfo Workstation Format String and Buffer Overflow Vulnerabilities | af854a3a-2127-422b-91ae-364c |
| ArcGIS Buffer Overflows and Format String Errors Let Local Users Gain Root Privileges - SecurityTracker | af854a3a-2127-422b-91ae-364c |
| Patches and Service Packs - ESRI Support | af854a3a-2127-422b-91ae-364c |
| www.digitalmunition.com/DMA%5B2005-0425a%5D.txt | af854a3a-2127-422b-91ae-364c |
| marc.info | af854a3a-2127-422b-91ae-364c |
| 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](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