



# CVE-2011-4714

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

## Summary

|                 |                                                                                                                                     |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------|
| CVE             | CVE-2011-4714                                                                                                                       |
| State           | PUBLISHED                                                                                                                           |
| Assigner        | mitre                                                                                                                               |
| Source Priority | CVE Program / NVD first with legacy fallback                                                                                        |
| Published       | 2011-12-08 19:55:08 UTC                                                                                                             |
| Updated         | 2026-04-29 01:13:23 UTC                                                                                                             |
| Description     | Directory traversal vulnerability in Virtual Vertex Muster before 6.20 allows remote attackers to read arbitrary files via a \.. (b |

## Risk And Classification

Primary CVSS: v2.0 5 from nvd@nist.gov

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

Problem Types: CWE-22 | n/a

## CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

None

Availability

None

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

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor  | Product | Version | Update | Edition | Language |
|-------------|---------|---------|---------|--------|---------|----------|
| Application | Vvertex | Muster  | All     | 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                                                                           |               |
| Muster Render Farm Management System Arbitrary File Download          |        | af854a3a-2127-422b-91ae-364da2661108 | <a href="http://www.exploit-db.com">www.exploit-db.com</a>                     |               |
| osvdb.org/77375                                                       |        | af854a3a-2127-422b-91ae-364da2661108 | <a href="http://osvdb.org">osvdb.org</a>                                       |               |
| Security Alerts - Secunia                                             |        | af854a3a-2127-422b-91ae-364da2661108 | <a href="http://secunia.com">secunia.com</a>                                   |               |
| Virtual Vertex Muster Web Interface Directory Traversal Vulnerability |        | af854a3a-2127-422b-91ae-364da2661108 | <a href="http://www.securityfocus.com">www.securityfocus.com</a>               |               |
| IBM X-Force Exchange                                                  |        | af854a3a-2127-422b-91ae-364da2661108 | <a href="http://exchange.xforce.ibmcloud.com">exchange.xforce.ibmcloud.com</a> |               |
| Risks in POS Systems: The Importance of a Security Assessment         |        | af854a3a-2127-422b-91ae-364da2661108 | <a href="http://www.security-assessment.com">www.security-assessment.com</a>   |               |
| CVE Program record                                                    |        | CVE.ORG                              | <a href="http://www.cve.org">www.cve.org</a>                                   |               |
| NVD vulnerability detail                                              |        | NVD                                  | <a href="http://nvd.nist.gov">nvd.nist.gov</a>                                 |               |
| <div><div></div><div></div></div>                                     |        |                                      |                                                                                |               |
| No vendor comments have been submitted for this CVE.                  |        |                                      |                                                                                |               |
|                                                                       |        |                                      |                                                                                |               |
| There are currently no legacy QID mappings associated with this CVE.  |        |                                      |                                                                                |               |