

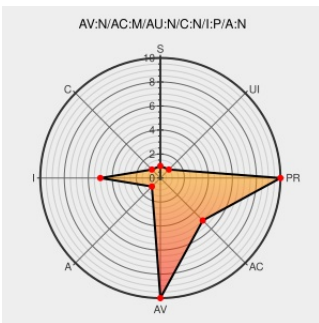


# CVE-2005-2981

Published on: 09/19/2005 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:28 PM UTC

## CVE-2005-2981

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Orion Application Server](#) from [Orionserver](#) contain the following vulnerability:

Cross-site scripting (XSS) vulnerability in Orion 1.3.8 and 1.4.5 allows remote attackers to inject arbitrary web script or HTML via the URL, which is not properly quoted in the resulting 404 error page.

CVE-2005-2981 has been assigned by [M](#) [cve@mitre.org](mailto:cve@mitre.org) to track the vulnerability

CVSS2 Score: **4.3 - MEDIUM**

**Access  
Vector**

**NETWORK**

**Access  
Complexity**

**MEDIUM**

**Authentication**

**NONE**

**Confidentiality  
Impact**

**NONE**

**Integrity  
Impact**

**PARTIAL**

**Availability  
Impact**

**NONE**

## CVE References

**Description**

**Tags**

**Link**

'404 error XSS' - MARC

[Third Party Advisory](#)

[marc.info](#)

[text/html](#)

[BUGTRAQ 20050914 404 error XSS](#)

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to [comment@cve.report](mailto:comment@cve.report).

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

| Type                                                           | Vendor                      | Product                                  | Version                   | Update | Edition | Language |
|----------------------------------------------------------------|-----------------------------|------------------------------------------|---------------------------|--------|---------|----------|
| Application                                                    | <a href="#">Orionserver</a> | <a href="#">Orion Application Server</a> | 1.3.8                     | All    | All     | All      |
| Application                                                    | <a href="#">Orionserver</a> | <a href="#">Orion Application Server</a> | 1.4.5                     | All    | All     | All      |
| Application                                                    | <a href="#">Orionserver</a> | <a href="#">Orion Application Server</a> | 1.3.8                     | All    | All     | All      |
| Application                                                    | <a href="#">Orionserver</a> | <a href="#">Orion Application Server</a> | 1.4.5                     | All    | All     | All      |
| cpe:2.3:a:orionserver:orion_application_server:1.3.8:****:***: |                             |                                          |                           |        |         |          |
| cpe:2.3:a:orionserver:orion_application_server:1.4.5:****:***: |                             |                                          |                           |        |         |          |
| cpe:2.3:a:orionserver:orion_application_server:1.3.8:****:***: |                             |                                          |                           |        |         |          |
| cpe:2.3:a:orionserver:orion_application_server:1.4.5:****:***: |                             |                                          |                           |        |         |          |
| No vendor comments have been submitted for this CVE            |                             |                                          |                           |        |         |          |
| <a href="#">← Previous ID</a>                                  |                             |                                          | <a href="#">Next ID →</a> |        |         |          |