



CVE-2006-0816

Published on: 03/24/2006 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:05 PM UTC

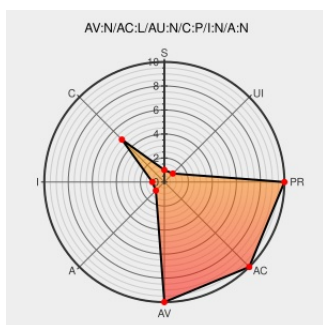
CVE-2006-0816

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



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

Orion Application Server before 2.0.7, when running on Windows, allows remote attackers to obtain the source code of JSP files via (1) . (dot) and (2) space characters in the extension of a URL.

CVE-2006-0816 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **5 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

NONE

Availability
Impact

NONE

CVE References

Description

Tags

Link

No Description Provided

Broken Link

www.osvdb.org

[OSVDB 24053](#)

Inactive Link

Not Archived

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

Broken Link

Third Party Advisory

www.vupen.com

[text/html](#)

[VUPEN ADV-2006-1055](#)

IBM X-Force Exchange

Third Party Advisory

VDB Entry

exchange.xforce.ibmcloud.com

[text/html](#)

[XF orion-jsp-source-disclosure\(25405\)](#)

Orion Application Server JSP Source Disclosure Vulnerability -
Secunia Research - Secunia

Third Party Advisory

web.archive.org

[MISC](#)
secunia.com/secunia_research/2006-

Secunia Research - Secunia	web.archive.org text/html	secunia.com/secunia_research/200611/advisory/
Orion Application Server JSP Source Disclosure Vulnerability	Third Party Advisory VDB Entry cve.report (archive) text/html	🌐 BID 17204
Orion Application Server JSP Source Disclosure Vulnerability - Advisories - Secunia	Third Party Advisory web.archive.org text/html	✖ SECUNIA 18950
Orion Application Server Discloses JSP Source Code to Remote Users - SecurityTracker	Third Party Advisory VDB Entry securitytracker.com text/html	🌐 SECTRAK 1015823
SecurityFocus	www.securityfocus.com text/html	🌐 BUGTRAQ 20060323 Secunia Research: Orion Application Server JSP Source Disclosure Vulnerability
Neohapsis Archives - Full Disclosure List - #1455 - [Full-disclosure] Secunia Research: Orion Application Server JSP Source Disclosure Vulnerability	Broken Link Third Party Advisory web.archive.org text/html Inactive Link Not Archived	🌐 FULLDISC 20060323 Secunia Research: Orion Application Server JSP Source Disclosure Vulnerability

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.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Orionserver	Orion Application Server	All	All	All	All
cpe:2.3:a:orionserver:orion_application_server:*****::						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2023  |

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](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)