

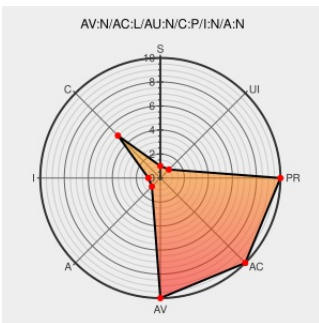


CVE-2002-1859

Published on: 12/31/2002 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:02 PM UTC

CVE-2002-1859

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

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

Orion Application Server 1.5.3, when running on Windows, allows remote attackers to retrieve files in the WEB-INF directory, which contains Java class files and configuration information, via a request to the WEB-INF directory with a trailing dot ("WEB-INF.").

CVE-2002-1859 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

ISS X-Force Database: webinf-dot-file-retrieval (9446): Multiple vendor /WEB-INF./ could allow an attacker to retrieve arbitrary files

Tags

[Patch](#)
[web.archive.org](#)
[text/html](#)
[Inactive Link](#) [Not Archived](#)

Link

[🌐 XF webinf-dot-file-retrieval\(9446\)](#)

Multiple Vendor WEB-INF Directory Contents Disclosure Vulnerability

[Third Party Advisory](#)
[VDB Entry](#)
[cve.report \(archive\)](#)
[text/html](#)

[🌐 BID 5119](#)

SecurityFocus HOME Mailing List: BugTraq

[Not Applicable](#)
[web.archive.org](#)
[text/html](#)
[Inactive Link](#) [Not Archived](#)

[🌐 BUGTRAQ 20020628 wp-02-0002: 'WEB-INF' Folder accessible in Multiple Web Application Servers](#)

[Vendor Advisory](#)
[www.westpoint.ltd.uk](#)

[🌐 MISC](#)
[www.westpoint.ltd.uk/advisories/wp-02-](#)

There are currently no QIDs associated with this CVE

Type	Vendor	Product	Version	Update	Edition	Language
Application	Orionserver	Orion Application Server	1.5.3	All	All	All
Application	Orionserver	Orion Application Server	1.5.3	All	All	All
cpe:2.3:a:orionserver:orion_application_server:1.5.3:****:***:						
cpe:2.3:a:orionserver:orion_application_server:1.5.3:****:***:						

← Previous ID

Next ID→