



# CVE-2002-1315

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

## Summary

<b>CVE</b>	CVE-2002-1315
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2002-11-29 05:00:00 UTC
<b>Updated</b>	2016-10-18 02:25:00 UTC
<b>Description</b>	Cross-site scripting (XSS) vulnerability in the Admin Server for iPlanet WebServer 4.x, up to SP11, allows remote attackers

## Risk And Classification

**Problem Types:** NVD-CWE-Other

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Iplanet</a>	<a href="#">Iplanet Web Server</a>	4.1	All	All	All
Application	<a href="#">Iplanet</a>	<a href="#">Iplanet Web Server</a>	4.1_sp1	All	All	All
Application	<a href="#">Iplanet</a>	<a href="#">Iplanet Web Server</a>	4.1_sp10	All	All	All
Application	<a href="#">Iplanet</a>	<a href="#">Iplanet Web Server</a>	4.1_sp11	All	All	All
Application	<a href="#">Iplanet</a>	<a href="#">Iplanet Web Server</a>	4.1_sp2	All	All	All
Application	<a href="#">Iplanet</a>	<a href="#">Iplanet Web Server</a>	4.1_sp3	All	All	All
Application	<a href="#">Iplanet</a>	<a href="#">Iplanet Web Server</a>	4.1_sp4	All	All	All
Application	<a href="#">Iplanet</a>	<a href="#">Iplanet Web Server</a>	4.1_sp5	All	All	All
Application	<a href="#">Iplanet</a>	<a href="#">Iplanet Web Server</a>	4.1_sp6	All	All	All
Application	<a href="#">Iplanet</a>	<a href="#">Iplanet Web Server</a>	4.1_sp7	All	All	All
Application	<a href="#">Iplanet</a>	<a href="#">Iplanet Web Server</a>	4.1_sp8	All	All	All
Application	<a href="#">Iplanet</a>	<a href="#">Iplanet Web Server</a>	4.1_sp9	All	All	All
Application	<a href="#">Iplanet</a>	<a href="#">Iplanet Web Server</a>	4.1	All	All	All
Application	<a href="#">Iplanet</a>	<a href="#">Iplanet Web Server</a>	4.1_sp1	All	All	All
Application	<a href="#">Iplanet</a>	<a href="#">Iplanet Web Server</a>	4.1_sp10	All	All	All
Application	<a href="#">Iplanet</a>	<a href="#">Iplanet Web Server</a>	4.1_sp11	All	All	All
Application	<a href="#">Iplanet</a>	<a href="#">Iplanet Web Server</a>	4.1_sp2	All	All	All

Application	<a href="#">Iplanet</a>	<a href="#">Iplanet Web Server</a>	4.1_sp3	All	All	All
Application	<a href="#">Iplanet</a>	<a href="#">Iplanet Web Server</a>	4.1_sp4	All	All	All
Application	<a href="#">Iplanet</a>	<a href="#">Iplanet Web Server</a>	4.1_sp5	All	All	All
Application	<a href="#">Iplanet</a>	<a href="#">Iplanet Web Server</a>	4.1_sp6	All	All	All
Application	<a href="#">Iplanet</a>	<a href="#">Iplanet Web Server</a>	4.1_sp7	All	All	All
Application	<a href="#">Iplanet</a>	<a href="#">Iplanet Web Server</a>	4.1_sp8	All	All	All
Application	<a href="#">Iplanet</a>	<a href="#">Iplanet Web Server</a>	4.1_sp9	All	All	All

## References

Reference	Source
20021119 iPlanet WebServer, remote root compromise	BUGTRAQ
20021118 iPlanet WebServer, remote root compromise	VULNWATCH
404 Not Found	MISC
iPlanet Admin Server Cross Site Scripting Vulnerability	BID
ISS X-Force Database: iplanet-admin-log-xss (10692): iPlanet (Sun ONE) Web Server admin error log cross-site scripting	XF
#49475: Security Vulnerabilities with Sun ONE Web Server 4.1SP11 and Earlier java.lang.NullPointerException	SUNALERT
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](#) 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](#) 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](#)**