



# CVE-2004-2763

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

## Summary

<b>CVE</b>	CVE-2004-2763
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2009-06-01 22:30:00 UTC
<b>Updated</b>	2009-06-02 04:00:00 UTC
<b>Description</b>	The default configuration of Sun ONE/iPlanet Web Server 4.1 SP1 through SP12 and 6.0 SP1 through SP5 responds to the

## Risk And Classification

### Problem Types: CWE-16

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Sun</a>	<a href="#">Iplanet Web Server</a>	4.1	sp1	All	All
Application	<a href="#">Sun</a>	<a href="#">Iplanet Web Server</a>	4.1	sp1	enterprise	All
Application	<a href="#">Sun</a>	<a href="#">Iplanet Web Server</a>	4.1	sp10	All	All
Application	<a href="#">Sun</a>	<a href="#">Iplanet Web Server</a>	4.1	sp10	enterprise	All
Application	<a href="#">Sun</a>	<a href="#">Iplanet Web Server</a>	4.1	sp11	All	All
Application	<a href="#">Sun</a>	<a href="#">Iplanet Web Server</a>	4.1	sp11	enterprise	All
Application	<a href="#">Sun</a>	<a href="#">Iplanet Web Server</a>	4.1	sp12	All	All
Application	<a href="#">Sun</a>	<a href="#">Iplanet Web Server</a>	4.1	sp12	enterprise	All
Application	<a href="#">Sun</a>	<a href="#">Iplanet Web Server</a>	4.1	sp2	All	All
Application	<a href="#">Sun</a>	<a href="#">Iplanet Web Server</a>	4.1	sp2	enterprise	All
Application	<a href="#">Sun</a>	<a href="#">Iplanet Web Server</a>	4.1	sp3	All	All
Application	<a href="#">Sun</a>	<a href="#">Iplanet Web Server</a>	4.1	sp3	enterprise	All
Application	<a href="#">Sun</a>	<a href="#">Iplanet Web Server</a>	4.1	sp4	All	All
Application	<a href="#">Sun</a>	<a href="#">Iplanet Web Server</a>	4.1	sp4	enterprise	All
Application	<a href="#">Sun</a>	<a href="#">Iplanet Web Server</a>	4.1	sp5	All	All
Application	<a href="#">Sun</a>	<a href="#">Iplanet Web Server</a>	4.1	sp5	enterprise	All
Application	<a href="#">Sun</a>	<a href="#">Iplanet Web Server</a>	4.1	sp6	All	All

Application	Sun	Iplanet Web Server	4.1	sp6	enterprise	All
Application	Sun	Iplanet Web Server	4.1	sp7	All	All
Application	Sun	Iplanet Web Server	4.1	sp7	enterprise	All
Application	Sun	Iplanet Web Server	4.1	sp8	All	All
Application	Sun	Iplanet Web Server	4.1	sp8	enterprise	All
Application	Sun	Iplanet Web Server	4.1	sp9	All	All
Application	Sun	Iplanet Web Server	4.1	sp9	enterprise	All
Application	Sun	Iplanet Web Server	6.0	sp1	All	All
Application	Sun	Iplanet Web Server	6.0	sp2	All	All
Application	Sun	Iplanet Web Server	6.0	sp3	All	All
Application	Sun	Iplanet Web Server	6.0	sp4	All	All
Application	Sun	Iplanet Web Server	6.0	sp5	All	All
Application	Sun	Iplanet Web Server	4.1	sp1	All	All
Application	Sun	Iplanet Web Server	4.1	sp1	enterprise	All
Application	Sun	Iplanet Web Server	4.1	sp10	All	All
Application	Sun	Iplanet Web Server	4.1	sp10	enterprise	All
Application	Sun	Iplanet Web Server	4.1	sp11	All	All
Application	Sun	Iplanet Web Server	4.1	sp11	enterprise	All
Application	Sun	Iplanet Web Server	4.1	sp12	All	All
Application	Sun	Iplanet Web Server	4.1	sp12	enterprise	All
Application	Sun	Iplanet Web Server	4.1	sp2	All	All
Application	Sun	Iplanet Web Server	4.1	sp2	enterprise	All
Application	Sun	Iplanet Web Server	4.1	sp3	All	All
Application	Sun	Iplanet Web Server	4.1	sp3	enterprise	All
Application	Sun	Iplanet Web Server	4.1	sp4	All	All
Application	Sun	Iplanet Web Server	4.1	sp4	enterprise	All
Application	Sun	Iplanet Web Server	4.1	sp5	All	All
Application	Sun	Iplanet Web Server	4.1	sp5	enterprise	All
Application	Sun	Iplanet Web Server	4.1	sp6	All	All
Application	Sun	Iplanet Web Server	4.1	sp6	enterprise	All
Application	Sun	Iplanet Web Server	4.1	sp7	All	All
Application	Sun	Iplanet Web Server	4.1	sp7	enterprise	All
Application	Sun	Iplanet Web Server	4.1	sp8	All	All
Application	Sun	Iplanet Web Server	4.1	sp8	enterprise	All
Application	Sun	Iplanet Web Server	4.1	sp9	All	All

Application	Sun	Iplanet Web Server	4.1	sp9	enterprise	All
Application	Sun	Iplanet Web Server	6.0	sp1	All	All
Application	Sun	Iplanet Web Server	6.0	sp2	All	All
Application	Sun	Iplanet Web Server	6.0	sp3	All	All
Application	Sun	Iplanet Web Server	6.0	sp4	All	All
Application	Sun	Iplanet Web Server	6.0	sp5	All	All
Application	Sun	One Web Server	4.1	All	All	All
Application	Sun	One Web Server	4.1	sp1	All	All
Application	Sun	One Web Server	4.1	sp10	All	All
Application	Sun	One Web Server	4.1	sp11	All	All
Application	Sun	One Web Server	4.1	sp12	All	All
Application	Sun	One Web Server	4.1	sp2	All	All
Application	Sun	One Web Server	4.1	sp3	All	All
Application	Sun	One Web Server	4.1	sp4	All	All
Application	Sun	One Web Server	4.1	sp5	All	All
Application	Sun	One Web Server	4.1	sp6	All	All
Application	Sun	One Web Server	4.1	sp7	All	All
Application	Sun	One Web Server	4.1	sp8	All	All
Application	Sun	One Web Server	4.1	sp9	All	All
Application	Sun	One Web Server	6.0	sp3	All	All
Application	Sun	One Web Server	6.0	sp4	All	All
Application	Sun	One Web Server	6.0	sp5	All	All
Application	Sun	One Web Server	6.1	sp1	All	All
Application	Sun	One Web Server	6.1	sp2	All	All
Application	Sun	One Web Server	4.1	All	All	All
Application	Sun	One Web Server	4.1	sp1	All	All
Application	Sun	One Web Server	4.1	sp10	All	All
Application	Sun	One Web Server	4.1	sp11	All	All
Application	Sun	One Web Server	4.1	sp12	All	All
Application	Sun	One Web Server	4.1	sp2	All	All
Application	Sun	One Web Server	4.1	sp3	All	All
Application	Sun	One Web Server	4.1	sp4	All	All
Application	Sun	One Web Server	4.1	sp5	All	All
Application	Sun	One Web Server	4.1	sp6	All	All
Application	Sun	One Web Server	4.1	sp7	All	All

Application	Sun	One Web Server	4.1	sp8	All	All
Application	Sun	One Web Server	4.1	sp9	All	All
Application	Sun	One Web Server	6.0	sp3	All	All
Application	Sun	One Web Server	6.0	sp4	All	All
Application	Sun	One Web Server	6.0	sp5	All	All
Application	Sun	One Web Server	6.1	sp1	All	All
Application	Sun	One Web Server	6.1	sp2	All	All

## References

Reference	Source	Link	Tags
RUS-CERT - Home	SUNALERT	<a href="https://archive.cert.uni-stuttgart.de">archive.cert.uni-stuttgart.de</a>	
Access denied   www.cgisecurity.com used Cloudflare to restrict access	MISC	<a href="https://www.cgisecurity.com">www.cgisecurity.com</a>	Exploit
Vulnerability Note VU#867593 - Web servers enable HTTP TRACE method by default	CERT-VN	<a href="https://www.kb.cert.org">www.kb.cert.org</a>	US Gov
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](https://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](https://mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://mitre.org/cve). This site includes MITRE data granted under the following [license](https://mitre.org/licenses).

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)