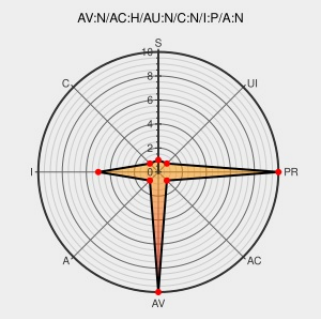
CVE-2003-1577

Published on: 02/05/2010 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:43 PM UTC

CVE-2003-1577

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of One Web Server from Sun contain the following vulnerability:

Sun ONE (aka iPlanet) Web Server 4.1 through SP12 and 6.0 through SP5, when DNS resolution is enabled for client IP addresses, allows remote attackers to inject arbitrary text into log files, and conduct cross-site scripting (XSS) attacks involving the iPlanet Log Analyzer, via an HTTP request in conjunction with a crafted DNS response, related to an "Inverse Lookup Log Corruption (ILLC)" issue, a different vulnerability than CVE-2002-1315 and CVE-2002-1316.

CVE-2003-1577 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 2.6 - LOW

Access Vector	Access Complexity	Authentication
NETWORK	HIGH	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
SecurityFocus	Exploit, www.securityfocus.com, text/html	BUGTRAQ 20030304 Log corruption on multiple webservers, log analyzers,...
IBM X-Force Exchange	exchange.xforce.ibmcloud.com, text/html	XF sunone-iplanetlog-xss(56632)
No Description Provided	Patch, Vendor Advisory, sunsolve.sun.com, Inactive Link, Not Archived	SUNALERT 201453

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	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	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	All	All	All
Application	Sun	One Web Server	6.0	sp1	All	All
Application	Sun	One Web Server	6.0	sp2	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	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	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	All	All	All
Application	Sun	One Web Server	6.0	sp1	All	All
Application	Sun	One Web Server	6.0	sp2	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	All	sp12	All	All
Application	Sun	One Web Server	All	sp5	All	All

cpe:2.3:a:sun:one_web_server:4.1:*:*:*:*:*:*:*:

cpe:2.3:a:sun:one_web_server:4.1:sp1:*:*:*:*:*:*:

cpe:2.3:a:sun:one_web_server:4.1:sp10:*:*:*:*:*:*:

cpe:2.3:a:sun:one_web_server:4.1:sp11:*:*:*:*:*:*:

cpe:2.3:a:sun:one_web_server:4.1:sp2:*:*:*:*:*:*:

cpe:2.3:a:sun:one_web_server:4.1:sp3:*:*:*:*:*:*:

cpe:2.3:a:sun:one_web_server:4.1:sp4:*:*:*:*:*:*:

cpe:2.3:a:sun:one_web_server:4.1:sp5:*:*:*:*:*:*:

cpe:2.3:a:sun:one_web_server:4.1:sp6:*:*:*:*:*:*:

cpe:2.3:a:sun:one_web_server:4.1:sp7:*:*:*:*:*:*:

cpe:2.3:a:sun:one_web_server:4.1:sp8:*:*:*:*:*:*:

cpe:2.3:a:sun:one_web_server:4.1:sp9:*:*:*:*:*:*:

cpe:2.3:a:sun:one_web_server:6.0:*:*:*:*:*:*:*:

cpe:2.3:a:sun:one_web_server:6.0:sp1:*:*:*:*:*:*:

cpe:2.3:a:sun:one_web_server:6.0:sp2:*:*:*:*:*:*:

cpe:2.3:a:sun:one_web_server:6.0:sp3:*:*:*:*:*:*:

cpe:2.3:a:sun:one_web_server:6.0:sp4:*:*:*:*:*:*:

cpe:2.3:a:sun:one_web_server:4.1:*:*:*:*:*:*:*:

cpe:2.3:a:sun:one_web_server:4.1:sp1:*:*:*:*:*:*:

cpe:2.3:a:sun:one_web_server:4.1:sp10:*:*:*:*:*:*:

cpe:2.3:a:sun:one_web_server:4.1:sp11:*:*:*:*:*:*:

cpe:2.3:a:sun:one_web_server:4.1:sp2:*:*:*:*:*:*:

cpe:2.3:a:sun:one_web_server:4.1:sp3:*:*:*:*:*:*:

cpe:2.3:a:sun:one_web_server:4.1:sp4:*:*:*:*:*:*:

cpe:2.3:a:sun:one_web_server:4.1:sp5:*:*:*:*:*:*:

cpe:2.3:a:sun:one_web_server:4.1:sp6:*:*:*:*:*:*:

cpe:2.3:a:sun:one_web_server:4.1:sp7:*:*:*:*:*:*:

cpe:2.3:a:sun:one_web_server:4.1:sp8:*:*:*:*:*:*:

cpe:2.3:a:sun:one_web_server:4.1:sp9:*:*:*:*:*:*:

cpe:2.3:a:sun:one_web_server:6.0:*:*:*:*:*:*:*:

cpe:2.3:a:sun:one_web_server:6.0:sp1:*:*:*:*:*:*:

cpe:2.3:a:sun:one_web_server:6.0:sp2:*:*:*:*:*:*:

cpe:2.3:a:sun:one_web_server:6.0:sp3:*:*:*:*:*:*:

cpe:2.3:a:sun:one_web_server:6.0:sp4:*:*:*:*:*:*:

cpe:2.3:a:sun:one_web_server:*:sp12:*:*:*:*:*:*:

cpe:2.3:a:sun:one_web_server:*:sp5:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→