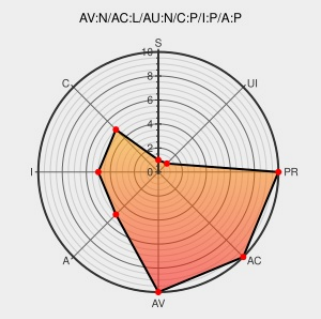
# CVE-2003-0151

Published on: 03/21/2003 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:45 PM UTC

## CVE-2003-0151

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




Certain versions of Weblogic Server from Bea contain the following vulnerability:

BEA WebLogic Server and Express 6.0 through 7.0 does not properly restrict access to certain internal servlets that perform administrative functions, which allows remote attackers to read arbitrary files or execute arbitrary code.

CVE-2003-0151 has been assigned by cve@mitre.org to track the vulnerability

### CVSS2 Score: 7.5 - HIGH

| Access Vector | Access Complexity | Authentication |
|---|---|---|
| NETWORK | LOW | NONE |
| **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| PARTIAL | PARTIAL | PARTIAL |

### CVE References

| Description | Tags | Link |
|---|---|---|
| BEA WebLogic Remote Unprivileged Administration Access Vulnerability | cve.report (archive) text/html | BID 7124 |
| Advisories & Notifications | dev2dev.bea.com text/html | CONFIRM dev2dev.bea.com/resourcelibrary/advisoriesnotifications/BEA03-28.jsp |
| Page not found – S21Sec | www.s21sec.com text/html Inactive Link Not Archived | MISC www.s21sec.com/en/avisos/s21sec-011-en.txt |
| No Description Provided | marc.info text/html | BUGTRAQ 20030317 SPI ADVISORY: Remote Administration of BEA WebLogic Server and Express |
| 'S21SEC-011 - Multiple vulnerabilities in BEA WebLogic Server' - MARC | marc.info text/html | BUGTRAQ 20030317 S21SEC-011 - Multiple vulnerabilities in BEA WebLogic Server |

BEA WebLogic Internal Servlet Input Validation Vulnerabilities

cve.report (archive) text/html

BID 7122

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 | Bea | Weblogic Server | 6.0 | All | All | All |
| Application | Bea | Weblogic Server | 6.0 | All | express | All |
| Application | Bea | Weblogic Server | 6.0 | sp1 | All | All |
| Application | Bea | Weblogic Server | 6.0 | sp1 | express | All |
| Application | Bea | Weblogic Server | 6.0 | sp2 | All | All |
| Application | Bea | Weblogic Server | 6.0 | sp2 | express | All |
| Application | Bea | Weblogic Server | 6.1 | All | All | All |
| Application | Bea | Weblogic Server | 6.1 | All | express | All |
| Application | Bea | Weblogic Server | 6.1 | sp1 | All | All |
| Application | Bea | Weblogic Server | 6.1 | sp1 | express | All |
| Application | Bea | Weblogic Server | 6.1 | sp2 | All | All |
| Application | Bea | Weblogic Server | 6.1 | sp2 | express | All |
| Application | Bea | Weblogic Server | 6.1 | sp3 | All | All |
| Application | Bea | Weblogic Server | 6.1 | sp3 | express | All |
| Application | Bea | Weblogic Server | 6.1 | sp4 | All | All |
| Application | Bea | Weblogic Server | 6.1 | sp4 | express | All |
| Application | Bea | Weblogic Server | 7.0 | All | All | All |
| Application | Bea | Weblogic Server | 7.0 | All | express | All |
| Application | Bea | Weblogic Server | 7.0 | sp1 | All | All |
| Application | Bea | Weblogic Server | 7.0 | sp1 | express | All |
| Application | Bea | Weblogic Server | 7.0 | sp2 | All | All |
| Application | Bea | Weblogic Server | 7.0 | sp2 | express | All |
| Application | Bea | Weblogic Server | 7.0.0.1 | All | All | All |
| Application | Bea | Weblogic Server | 7.0.0.1 | All | express | All |
| Application | Bea | Weblogic Server | 7.0.0.1 | sp1 | All | All |
| Application | Bea | Weblogic Server | 7.0.0.1 | sp1 | express | All |

| | | | | | | |
|---|---|---|---|---|---|---|
| Application | Bea | Weblogic Server | 7.0.0.1 | sp2 | All | All |
| Application | Bea | Weblogic Server | 7.0.0.1 | sp2 | express | All |
| Application | Bea | Weblogic Server | 6.0 | All | All | All |
| Application | Bea | Weblogic Server | 6.0 | All | express | All |
| Application | Bea | Weblogic Server | 6.0 | sp1 | All | All |
| Application | Bea | Weblogic Server | 6.0 | sp1 | express | All |
| Application | Bea | Weblogic Server | 6.0 | sp2 | All | All |
| Application | Bea | Weblogic Server | 6.0 | sp2 | express | All |
| Application | Bea | Weblogic Server | 6.1 | All | All | All |
| Application | Bea | Weblogic Server | 6.1 | All | express | All |
| Application | Bea | Weblogic Server | 6.1 | sp1 | All | All |
| Application | Bea | Weblogic Server | 6.1 | sp1 | express | All |
| Application | Bea | Weblogic Server | 6.1 | sp2 | All | All |
| Application | Bea | Weblogic Server | 6.1 | sp2 | express | All |
| Application | Bea | Weblogic Server | 6.1 | sp3 | All | All |
| Application | Bea | Weblogic Server | 6.1 | sp3 | express | All |
| Application | Bea | Weblogic Server | 6.1 | sp4 | All | All |
| Application | Bea | Weblogic Server | 6.1 | sp4 | express | All |
| Application | Bea | Weblogic Server | 7.0 | All | All | All |
| Application | Bea | Weblogic Server | 7.0 | All | express | All |
| Application | Bea | Weblogic Server | 7.0 | sp1 | All | All |
| Application | Bea | Weblogic Server | 7.0 | sp1 | express | All |
| Application | Bea | Weblogic Server | 7.0 | sp2 | All | All |
| Application | Bea | Weblogic Server | 7.0 | sp2 | express | All |
| Application | Bea | Weblogic Server | 7.0.0.1 | All | All | All |
| Application | Bea | Weblogic Server | 7.0.0.1 | All | express | All |
| Application | Bea | Weblogic Server | 7.0.0.1 | sp1 | All | All |
| Application | Bea | Weblogic Server | 7.0.0.1 | sp1 | express | All |
| Application | Bea | Weblogic Server | 7.0.0.1 | sp2 | All | All |
| Application | Bea | Weblogic Server | 7.0.0.1 | sp2 | express | All |

cpe:2.3:a:bea:weblogic_server:6.0:*:*:*:*:*:*:*:

cpe:2.3:a:bea:weblogic_server:6.0:*:express:*:*:*:*:*:

cpe:2.3:a:bea:weblogic_server:6.0:sp1:*:*:*:*:*:*:

cpe:2.3:a:bea:weblogic_server:6.0:sp1:express:*:*:*:*:*:

cpe:2.3:a:bea:weblogic_server:6.0:sp2:*:*:*:*:*:*:

cpe:2.3:a:bea:weblogic_server:6.0:sp2:express:*:*:*:*:*:

cpe:2.3:a:bea:weblogic_server:6.1:*:*:*:*:*:*:*:

cpe:2.3:a:bea:weblogic_server:6.1:*:express:*:*:*:*:*:

cpe:2.3:a:bea:weblogic_server:6.1:sp1:*:*:*:*:*:*:

cpe:2.3:a:bea:weblogic_server:6.1:sp1:express:*:*:*:*:*:

cpe:2.3:a:bea:weblogic_server:6.1:sp2:*:*:*:*:*:*:

cpe:2.3:a:bea:weblogic_server:6.1:sp2:express:*:*:*:*:*:

cpe:2.3:a:bea:weblogic_server:6.1:sp3:*:*:*:*:*:*:

cpe:2.3:a:bea:weblogic_server:6.1:sp3:express:*:*:*:*:*:

cpe:2.3:a:bea:weblogic_server:6.1:sp4:*:*:*:*:*:*:

cpe:2.3:a:bea:weblogic_server:6.1:sp4:express:*:*:*:*:*:

cpe:2.3:a:bea:weblogic_server:7.0:*:*:*:*:*:*:*:

cpe:2.3:a:bea:weblogic_server:7.0:*:express:*:*:*:*:*:

cpe:2.3:a:bea:weblogic_server:7.0:sp1:*:*:*:*:*:*:

cpe:2.3:a:bea:weblogic_server:7.0:sp1:express:*:*:*:*:*:

cpe:2.3:a:bea:weblogic_server:7.0:sp2:*:*:*:*:*:*:

cpe:2.3:a:bea:weblogic_server:7.0:sp2:express:*:*:*:*:*:

cpe:2.3:a:bea:weblogic_server:7.0.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:bea:weblogic_server:7.0.0.1:*:express:*:*:*:*:*:

cpe:2.3:a:bea:weblogic_server:7.0.0.1:sp1:*:*:*:*:*:*:

cpe:2.3:a:bea:weblogic_server:7.0.0.1:sp1:express:*:*:*:*:*:

cpe:2.3:a:bea:weblogic_server:7.0.0.1:sp2:*:*:*:*:*:*:

cpe:2.3:a:bea:weblogic_server:7.0.0.1:sp2:express:*:*:*:*:*:

cpe:2.3:a:bea:weblogic_server:6.0:*:*:*:*:*:*:*:

cpe:2.3:a:bea:weblogic_server:6.0:*:express:*:*:*:*:*:

cpe:2.3:a:bea:weblogic_server:6.0:sp1:*:*:*:*:*:*:

cpe:2.3:a:bea:weblogic_server:6.0:sp1:express:*:*:*:*:*:

cpe:2.3:a:bea:weblogic_server:6.0:sp2:*:*:*:*:*:*:

cpe:2.3:a:bea:weblogic_server:6.0:sp2:express:*:*:*:*:*:

cpe:2.3:a:bea:weblogic_server:6.1:*:*:*:*:*:*:*:

cpe:2.3:a:bea:weblogic_server:6.1:*:express:*:*:*:*:*:

cpe:2.3:a:bea:weblogic_server:6.1:sp1:*:*:*:*:*:*:

cpe:2.3:a:bea:weblogic_server:6.1:sp1:express:*:*:*:*:*:

cpe:2.3:a:bea:weblogic_server:6.1:sp2:*:*:*:*:*:*:

cpe:2.3:a:bea:weblogic_server:6.1:sp2:express:*:*:*:*:*:

cpe:2.3:a:bea:weblogic_server:6.1:sp3:*:*:*:*:*:*:

cpe:2.3:a:bea:weblogic_server:6.1:sp3:express:*:*:*:*:*:

cpe:2.3:a:bea:weblogic_server:6.1:sp4:*:*:*:*:*:*:

cpe:2.3:a:bea:weblogic_server:6.1:sp4:express:*:*:*:*:*:

cpe:2.3:a:bea:weblogic_server:7.0:*:*:*:*:*:*:*:

cpe:2.3:a:bea:weblogic_server:7.0:*:express:*:*:*:*:*:

cpe:2.3:a:bea:weblogic_server:7.0:sp1:*:*:*:*:*:*:

cpe:2.3:a:bea:weblogic_server:7.0:sp1:express:*:*:*:*:*:

cpe:2.3:a:bea:weblogic_server:7.0:sp2:*:*:*:*:*:*:

cpe:2.3:a:bea:weblogic_server:7.0:sp2:express:*:*:*:*:*:

cpe:2.3:a:bea:weblogic_server:7.0.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:bea:weblogic_server:7.0.0.1:*:express:*:*:*:*:*:

cpe:2.3:a:bea:weblogic_server:7.0.0.1:sp1:*:*:*:*:*:*:

cpe:2.3:a:bea:weblogic_server:7.0.0.1:sp1:express:*:*:*:*:*:

cpe:2.3:a:bea:weblogic_server:7.0.0.1:sp2:*:*:*:*:*:*:

cpe:2.3:a:bea:weblogic_server:7.0.0.1:sp2:express:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

**CVE.report and Source URL Uptime Status status.cve.report**