

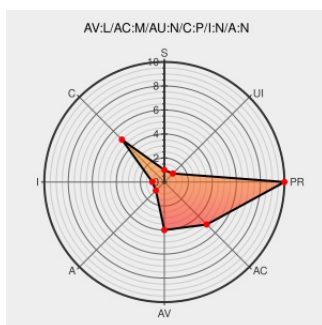


CVE-2010-1651

Published on: 04/30/2010 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:05 PM UTC

CVE-2010-1651

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

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

IBM WebSphere Application Server (WAS) 6.1.x before 6.1.0.31 and 7.0.x before 7.0.0.11, when Basic authentication and SIP tracing (aka full trace logging for SIP) are enabled, logs the entirety of all inbound and outbound SIP messages, which allows local users to obtain sensitive information by reading the trace log.

CVE-2010-1651 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **1.9 - LOW**

Access
Vector

LOCAL

Access
Complexity

MEDIUM

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

NONE

Availability
Impact

NONE

CVE References

Description

Tags

Link

IBM PM08892: SIP logging does not support hiding specific header fields - United States

[www-01.ibm.com](#)
text/html

[AIXAPAR PM08892](#)

No Description Provided

[www.osvdb.org](#)

[OSVDB 65437](#)

Inactive Link Not Archived

IBM WebSphere Application Server Multiple Vulnerabilities - Advisories - Community

[web.archive.org](#)
text/html

[SECUNIA 40096](#)

IBM X-Force Exchange

[exchange.xforce.ibmcloud.com](#)
text/html

[XF ibm-was-trace-information-disclosure\(58324\)](#)

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

[www.vupen.com](#)
text/html

[VUPEN ADV-2010-1411](#)

IBM PM12247: SHIP APAR FIXES FOR H28W610 FIX PACK 6.1.0.31. - United States	Patch www-01.ibm.com text/html	 AIXAPAR PM12247
IBM WebSphere Application Server for z/OS Multiple Vulnerabilities - Advisories - Community	Vendor Advisory web.archive.org text/html	 SECUNIA 39628
IBM PM15829: SHIP APAR FIXES FOR H28W700 FIX PACK 7.0.0.11. - United States	www-01.ibm.com text/html	 AIXAPAR PM15829

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	Ibm	Websphere Application Server	6.1	All	All	All
Application	Ibm	Websphere Application Server	6.1.0	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.0	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.1	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.10	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.11	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.12	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.13	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.14	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.15	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.16	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.17	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.18	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.19	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.2	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.20	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.21	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.22	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.23	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.24	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.25	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.26	All	All	All

[illegible]

Application	lbn	Websphere Application Server	6.1.0.19	All	All	All
Application	lbn	Websphere Application Server	6.1.0.2	All	All	All
Application	lbn	Websphere Application Server	6.1.0.20	All	All	All
Application	lbn	Websphere Application Server	6.1.0.21	All	All	All
Application	lbn	Websphere Application Server	6.1.0.22	All	All	All
Application	lbn	Websphere Application Server	6.1.0.23	All	All	All
Application	lbn	Websphere Application Server	6.1.0.24	All	All	All
Application	lbn	Websphere Application Server	6.1.0.25	All	All	All
Application	lbn	Websphere Application Server	6.1.0.26	All	All	All
Application	lbn	Websphere Application Server	6.1.0.27	All	All	All
Application	lbn	Websphere Application Server	6.1.0.29	All	All	All
Application	lbn	Websphere Application Server	6.1.0.3	All	All	All
Application	lbn	Websphere Application Server	6.1.0.4	All	All	All
Application	lbn	Websphere Application Server	6.1.0.5	All	All	All
Application	lbn	Websphere Application Server	6.1.0.6	All	All	All
Application	lbn	Websphere Application Server	6.1.0.7	All	All	All
Application	lbn	Websphere Application Server	6.1.0.8	All	All	All
Application	lbn	Websphere Application Server	6.1.0.9	All	All	All
Application	lbn	Websphere Application Server	6.1.1	All	All	All
Application	lbn	Websphere Application Server	6.1.13	All	All	All
Application	lbn	Websphere Application Server	6.1.14	All	All	All
Application	lbn	Websphere Application Server	6.1.3	All	All	All
Application	lbn	Websphere Application Server	6.1.5	All	All	All
Application	lbn	Websphere Application Server	6.1.6	All	All	All
Application	lbn	Websphere Application Server	6.1.7	All	All	All
Application	lbn	Websphere Application Server	7.0	All	All	All
Application	lbn	Websphere Application Server	7.0.0.1	All	All	All
Application	lbn	Websphere Application Server	7.0.0.3	All	All	All
Application	lbn	Websphere Application Server	7.0.0.5	All	All	All
Application	lbn	Websphere Application Server	7.0.0.7	All	All	All
Application	lbn	Websphere Application Server	7.0.0.9	All	All	All
Operating System	lbn	Z/os	All	All	All	All
Operating System	lbn	Z/os	All	All	All	All
Operating System	lbn	Z/os	All	All	All	All

cpe:2.3:a:ibm:websphere_application_server:6.1:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:6.1.0:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.0:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.1:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.10:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.11:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.12:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.13:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.14:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.15:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.16:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.17:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.18:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.19:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.2:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.20:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.21:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.22:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.23:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.24:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.25:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.26:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.27:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.29:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.3:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.4:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.5:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.6:*:*:*:*:*:

```
cpe:2.3:a:ibm:websphere_application_server:6.1.0.7:*:*:*:*:*:
```

```
cpe:2.3:a:ibm:websphere_application_server:6.1.0.8:*:*:*:*:*:
```

```
cpe:2.3:a:ibm:websphere_application_server:6.1.0.9:*:*:*:*:*:
```

```
cpe:2.3:a:ibm:websphere_application_server:6.1.1:*:*:*:*:*:*:
```

```
cpe:2.3:a:ibm:websphere_application_server:6.1.13:::*:*:*:*:*:
```

```
cpe:2.3:a:ibm:websphere_application_server:6.1.14:::*:*:*:*:*:
```

```
cpe:2.3:a:ibm:websphere_application_server:6.1.3:*:*:*:*:*:
```

```
cpe:2.3:a:ibm:websphere_application_server:6.1.5:*:*:*:*:*:
```

```
cpe:2.3:a:ibm:websphere_application_server:6.1.6:*:*:*:*:*:
```

```
cpe:2.3:a:ibm:websphere_application_server:6.1.7:*:*:*:*:*:
```

```
cpe:2.3:a:ibm:websphere_application_server:7.0:*:*:*:*:*:*
```

```
cpe:2.3:a:ibm:websphere_application_server:7.0.0.1:*.~*~*~*~*~*~*
```

```
cpe:2.3:a:ibm:websphere_application_server:7.0.0.3:*:*:*:*:*:
```

```
cpe:2.3:a:ibm:websphere_application_server:7.0.0.5:*:*:*:*:*:
```

```
cpe:2.3:a:ibm:websphere_application_server:7.0.0.7:*:*:*:*:*:
```

```
cpe:2.3:a:ibm:websphere_application_server:7.0.0.9:*:*:*:*:*:
```

```
cpe:2.3:a:ibm:websphere_application_server:6.1:::.*:.*:.*:.*:.*:.*:.*
```

```
cpe:2.3:a:ibm:websphere_application_server:6.1.0:*:*:*:*:*:*:
```

```
cpe:2.3:a:ibm:websphere_application_server:6.1.0.0:*:*:*:*:*:
```

```
cpe:2.3:a:ibm:websphere_application_server:6.1.0.1:*:*:*:*:*:
```

```
cpe:2.3:a:ibm:websphere_application_server:6.1.0.10:*:*:*:*:*:
```

```
cpe:2.3:a:ibm:websphere_application_server:6.1.0.11:::*:*:*:*:
```

```
cpe:2.3:a:ibm:websphere_application_server:6.1.0.12:*:*:*:*:*:
```

```
cpe:2.3:a:ibm:websphere_application_server:6.1.0.13:*:*:*:*:*:
```

```
cpe:2.3:a:ibm:websphere_application_server:6.1.0.14:*:*:*:*:*:
```

```
cpe:2.3:a:ibm:websphere_application_server:6.1.0.15:*:*:*:*:*:
```

```
cpe:2.3:a:ibm:websphere_application_server:6.1.0.16:*:*:*:*:*:
```

```
cpe:2.3:a:ibm:websphere_application_server:6.1.0.17:*:*:*:*:*.*
```

```
cpe:2.3:a:ibm:websphere_application_server:6.1.0.18:*:*:*:*:*:
```

```
cpe:2.3:a:ibm:websphere_application_server:6.1.0.19:::*:*:*:*:
```

```
cpe:2.3:a:ibm:websphere_application_server:6.1.0.2:*:*:*:*:*:
```

```
cpe:2.3:a:ibm:websphere_application_server:6.1.0.20:*:*:*:*:*:
```

```
cpe:2.3:a:ibm:websphere_application_server:6.1.0.21:*:*:*:*:*:
```

```
cpe:2.3:a:ibm:websphere_application_server:6.1.0.22:::*:*:*:*:*:
```

```
cpe:2.3:a:ibm:websphere_application_server:6.1.0.23:::*:*:*:*:*
```

```
cpe:2.3:a:ibm:websphere_application_server:6.1.0.24:::*:*:*:*:*
```

```
cpe:2.3:a:ibm:websphere_application_server:6.1.0.25:*:*:*:*:*:
```

```
cpe:2.3:a:ibm:websphere_application_server:6.1.0.26:*:*:*:*:*:
```

```
cpe:2.3:a:ibm:websphere_application_server:6.1.0.27:*:*:*:*:*.*
```

```
cpe:2.3:a:ibm:websphere_application_server:6.1.0.29:::*:*:*:*.*
```

```
cpe:2.3:a:ibm:websphere_application_server:6.1.0.3:*.~*~*~*~*~*~*
```

```
cpe:2.3:a:ibm:websphere_application_server:6.1.0.4:*.~*~*~*~*~*~*
```

```
cpe:2.3:a:ibm:websphere_application_server:6.1.0.5:*:*:*:*:*.*
```

```
cpe:2.3:a:ibm:websphere_application_server:6.1.0.6:*:*:*:*:*.*
```

```
cpe:2.3:a:ibm:websphere_application_server:6.1.0.7:*:*:*:*:*:
```

```
cpe:2.3:a:ibm:websphere_application_server:6.1.0.8:*.~*~*~*~*~*~*
```

```
cpe:2.3:a:ibm:websphere_application_server:6.1.0.9:*.~*~*~*~*~*~*
```

```
cpe:2.3:a:ibm:websphere_application_server:6.1.1:*:*:*:*:*.*
```

```
cpe:2.3:a:ibm:websphere_application_server:6.1.13:::*:*:*.*
```

```
cpe:2.3:a:ibm:websphere_application_server:6.1.14:*:*:*:*.*.*
```

```
cpe:2.3:a:ibm:websphere_application_server:6.1.3:*:*:*:*:*.*
```

```
cpe:2.3:a:ibm:websphere application server:6.1.5:*. *. *. *. *. *
```

```
cpe:2.3:a:ibm:websphere_application_server:6.1.6:*:*:*:*:*.*
```

```
cpe:2.3:a:ibm:websphere_application_server:6.1.7:*:*:*:*:*.*
```

```
cpe:2.3:a:ibm:websphere_application_server:7.0:*:*:*:*:*.*
```

```
cpe:2.3:a:ibm:websphere application server:7.0.0.1:*.~*~*~*~*~*~*
```

```
cpe:2.3:a:ibm:websphere application server:7.0.0.3:*.~*~*~*~*~*~*
```

cpe:2.3:a:ibm:websphere_application_server:7.0.0.5:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.7:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.9:*:*:*:*:*:
cpe:2.3:o:ibm:z/os:*:*:*:*:*:
cpe:2.3:o:ibm:z/Vos:*:*:*:*:*:
cpe:2.3:o:ibm:z/Vos:*:*:*:*:*:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)