



CVE-2010-2327

Published on: 06/18/2010 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:09 PM UTC

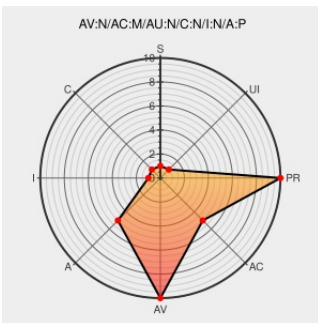
CVE-2010-2327

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



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

mod_ibm_ssl in IBM HTTP Server 6.0 before 6.0.2.43, 6.1 before 6.1.0.33, and 7.0 before 7.0.0.11, as used in IBM WebSphere Application Server (WAS) on z/OS, does not properly handle a large HTTP request body in uploading over SSL, which might allow remote attackers to cause a denial of service (daemon fail) via an upload.

CVE-2010-2327 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **4.3 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
IBM PM15830: SHIP APAR FIXES FOR H28W700 FIX PACK 7.0.0.11. - United States	www-01.ibm.com text/html	AIXAPAR PM15830
IBM WebSphere Application Server Multiple Vulnerabilities - Advisories - Community	Vendor Advisory web.archive.org text/html	SECUNIA 40096
No Description Provided	www.osvdb.org Inactive Link Not Archived	OSVDB 65439
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	Vendor Advisory www.vupen.com text/html	VUPEN ADV-2010-1411

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	6.0	All	All	All
Application	Ibm	Websphere Application Server	6.0.0.1	All	All	All
Application	Ibm	Websphere Application Server	6.0.0.2	All	All	All
Application	Ibm	Websphere Application Server	6.0.0.3	All	All	All
Application	Ibm	Websphere Application Server	6.0.1	All	All	All
Application	Ibm	Websphere Application Server	6.0.1.2	All	All	All
Application	Ibm	Websphere Application Server	6.0.2	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.1	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.11	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.13	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.15	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.17	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.19	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.21	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.23	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.25	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.27	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.29	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.3	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.31	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.33	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.35	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.37	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.39	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.41	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.5	All	All	All

[illegible]

[illegible]

Application	Ibm	Websphere Application Server	6.1.0.3	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.31	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.5	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.7	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.9	All	All	All
Application	Ibm	Websphere Application Server	7.0	All	All	All
Application	Ibm	Websphere Application Server	7.0.0.1	All	All	All
Application	Ibm	Websphere Application Server	7.0.0.3	All	All	All
Application	Ibm	Websphere Application Server	7.0.0.5	All	All	All
Application	Ibm	Websphere Application Server	7.0.0.7	All	All	All
Application	Ibm	Websphere Application Server	7.0.0.9	All	All	All
Operating System	Ibm	Z/os	All	All	All	All
Operating System	Ibm	Z/os	All	All	All	All
Operating System	Ibm	Z/os	All	All	All	All
cpe:2.3:a:ibm:websphere_application_server:6.0:*:*:*:*:*.*:						
cpe:2.3:a:ibm:websphere_application_server:6.0.0.1:*:*:*:*:*.*:						
cpe:2.3:a:ibm:websphere_application_server:6.0.0.2:*:*:*:*:*.*:						
cpe:2.3:a:ibm:websphere_application_server:6.0.0.3:*:*:*:*:*.*:						
cpe:2.3:a:ibm:websphere_application_server:6.0.1:*:*:*:*:*.*:						
cpe:2.3:a:ibm:websphere_application_server:6.0.1.2:*:*:*:*:*.*:						
cpe:2.3:a:ibm:websphere_application_server:6.0.2:*:*:*:*:*.*:						
cpe:2.3:a:ibm:websphere_application_server:6.0.2.1:*:*:*:*:*.*:						
cpe:2.3:a:ibm:websphere_application_server:6.0.2.11:*:*:*:*:*.*:						
cpe:2.3:a:ibm:websphere_application_server:6.0.2.13:*:*:*:*:*.*:						
cpe:2.3:a:ibm:websphere_application_server:6.0.2.15:*:*:*:*:*.*:						
cpe:2.3:a:ibm:websphere_application_server:6.0.2.17:*:*:*:*:*.*:						
cpe:2.3:a:ibm:websphere_application_server:6.0.2.19:*:*:*:*:*.*:						
cpe:2.3:a:ibm:websphere_application_server:6.0.2.21:*:*:*:*:*.*:						
cpe:2.3:a:ibm:websphere_application_server:6.0.2.23:*:*:*:*:*.*:						
cpe:2.3:a:ibm:websphere_application_server:6.0.2.25:*:*:*:*:*.*:						

cpe:2.3:a:ibm:websphere_application_server:6.0.2.27:*****:
cpe:2.3:a:ibm:websphere_application_server:6.0.2.29:*****:
cpe:2.3:a:ibm:websphere_application_server:6.0.2.3:*****:
cpe:2.3:a:ibm:websphere_application_server:6.0.2.31:*****:
cpe:2.3:a:ibm:websphere_application_server:6.0.2.33:*****:
cpe:2.3:a:ibm:websphere_application_server:6.0.2.35:*****:
cpe:2.3:a:ibm:websphere_application_server:6.0.2.37:*****:
cpe:2.3:a:ibm:websphere_application_server:6.0.2.39:*****:
cpe:2.3:a:ibm:websphere_application_server:6.0.2.41:*****:
cpe:2.3:a:ibm:websphere_application_server:6.0.2.5:*****:
cpe:2.3:a:ibm:websphere_application_server:6.0.2.7:*****:
cpe:2.3:a:ibm:websphere_application_server:6.0.2.9:*****:
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:6.1.0.11:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.13:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.15:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.17:*****:
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:6.1.0.21:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.23:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.25:*****:
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:6.1.0.31:*****:*
cpe:2.3:a:ibm:websphere_application_server:6.1.0.5:*****:*
cpe:2.3:a:ibm:websphere_application_server:6.1.0.7:*****:*
cpe:2.3:a:ibm:websphere_application_server:6.1.0.9:*****:*
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:6.0:*****:*
cpe:2.3:a:ibm:websphere_application_server:6.0.0.1:*****:*
cpe:2.3:a:ibm:websphere_application_server:6.0.0.2:*****:*
cpe:2.3:a:ibm:websphere_application_server:6.0.0.3:*****:*
cpe:2.3:a:ibm:websphere_application_server:6.0.1:*****:*
cpe:2.3:a:ibm:websphere_application_server:6.0.1.2:*****:*
cpe:2.3:a:ibm:websphere_application_server:6.0.2:*****:*
cpe:2.3:a:ibm:websphere_application_server:6.0.2.1:*****:*
cpe:2.3:a:ibm:websphere_application_server:6.0.2.11:*****:*
cpe:2.3:a:ibm:websphere_application_server:6.0.2.13:*****:*
cpe:2.3:a:ibm:websphere_application_server:6.0.2.15:*****:*
cpe:2.3:a:ibm:websphere_application_server:6.0.2.17:*****:*
cpe:2.3:a:ibm:websphere_application_server:6.0.2.19:*****:*
cpe:2.3:a:ibm:websphere_application_server:6.0.2.21:*****:*
cpe:2.3:a:ibm:websphere_application_server:6.0.2.23:*****:*
cpe:2.3:a:ibm:websphere_application_server:6.0.2.25:*****:*
cpe:2.3:a:ibm:websphere_application_server:6.0.2.27:*****:*
cpe:2.3:a:ibm:websphere_application_server:6.0.2.29:*****:*
cpe:2.3:a:ibm:websphere_application_server:6.0.2.3:*****:*

cpe:2.3:a:ibm:websphere_application_server:6.0.2.31:*****:
cpe:2.3:a:ibm:websphere_application_server:6.0.2.33:*****:
cpe:2.3:a:ibm:websphere_application_server:6.0.2.35:*****:
cpe:2.3:a:ibm:websphere_application_server:6.0.2.37:*****:
cpe:2.3:a:ibm:websphere_application_server:6.0.2.39:*****:
cpe:2.3:a:ibm:websphere_application_server:6.0.2.41:*****:
cpe:2.3:a:ibm:websphere_application_server:6.0.2.5:*****:
cpe:2.3:a:ibm:websphere_application_server:6.0.2.7:*****:
cpe:2.3:a:ibm:websphere_application_server:6.0.2.9:*****:
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:6.1.0.11:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.13:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.15:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.17:*****:
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:6.1.0.21:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.23:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.25:*****:
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:6.1.0.31:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.5:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.7:*****:

cpe:2.3:a:ibm:websphere_application_server:6.1.0.9:*****:
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/os:*****:
cpe:2.3:o:ibm:z/os:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)