



CVE-2021-29736

Published on: 07/30/2021 12:00:00 AM UTC

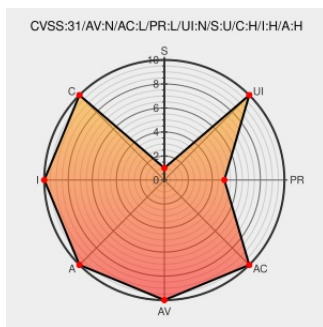
Last Modified on: 08/05/2021 03:24:00 PM UTC

CVE-2021-29736

[Source: Mitre](#)

[Source: Nist](#)

[Print: PDF](#)



Certain versions of **Hp-ux** from **Hp** contain the following vulnerability:

IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 could allow a remote user to gain elevated privileges on the system. IBM X-Force ID: 201300.

CVE-2021-29736 has been assigned by psirt@us.ibm.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **IBM - WebSphere Application Server** version **7.0**

Affected Vendor/Software: **IBM - WebSphere Application Server** version **8.0**

Affected Vendor/Software: **IBM - WebSphere Application Server** version **8.5**

Affected Vendor/Software: **IBM - WebSphere Application Server** version **9.0**



CVSS3 Score: **8.8 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **6.5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Security Bulletin: WebSphere Application Server is vulnerable to a Privilege Escalation vulnerability (CVE-2021-29736)	www.ibm.com text/html	 CONFIRM www.ibm.com/support/pages/node/6476678
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	 XF ibm-was-cve202129736-priv-escalation (201300)

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.

Related QID Numbers

375780 IBM WebSphere Application Server Privilege Escalation Vulnerability (6476678)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Hp	Hp-ux	-	All	All	All
Operating System	Ibm	Aix	-	All	All	All
Operating System	Ibm	I	-	All	All	All
Application	Ibm	Websphere Application Server	All	All	All	All
Application	Ibm	Websphere Application Server	All	All	All	All
Application	Ibm	Websphere Application Server	All	All	All	All
Application	Ibm	Websphere Application Server	All	All	All	All
Operating System	Ibm	Z/os	-	All	All	All
Operating System	Linux	Linux Kernel	-	All	All	All
Operating System	Microsoft	Windows	-	All	All	All
Operating System	Oracle	Solaris	-	All	All	All

`cpe:2.3:o:hp:hp-ux:-:*:*:*:*:*:`

`cpe:2.3:o:ibm:aix:-:*:*:*:*:*:`




`cpe:2.3:o:ibm:i:-:*:*:*:*:*:`

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

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

cpe:2.3:a:ibm:websphere_application_server:*:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:*:*:*:*:*:*:
cpe:2.3:o:ibm:zVos:-:*:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:-:*:*:*:*:*:*:
cpe:2.3:o:microsoft:windows:-:*:*:*:*:*:*:
cpe:2.3:o:oracle:solaris:-:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions		
Source	Title	Posted (UTC)
 @knaepp	PH34690:Privilege Escalation Vulnerability in WebSphere Application Server (CVE-2021-29736 CVSS 5.0) tinyurl.com/ydjs69ym	2021-07-29 14:55:02
 @CVEreport	CVE-2021-29736 : #IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 could allow a remote user to gain elevate... twitter.com/i/web/status/1...	2021-07-30 11:18:14
 /r/sysadmin	McAfee.McAfee Policy Auditor has many vulnerability reports	2021-08-02 07:58:19

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2021   |

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](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

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