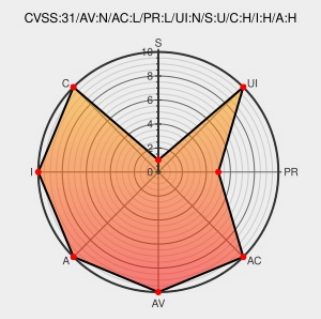
CVE-2021-20517

Published on: 06/07/2021 12:00:00 AM UTC

Last Modified on: 06/10/2021 06:02:00 PM UTC

CVE-2021-20517

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



Certain versions of Websphere Application Server Nd from Ibm contain the following vulnerability:

IBM WebSphere Application Server Network Deployment 8.5 and 9.0 could allow a remote authenticated attacker to traverse directories. An attacker could send a specially-crafted URL request containing "dot dot" sequences (/../) to read and delete arbitrary files on the system. IBM X-Force ID: 198435.

CVE-2021-20517 has been assigned by psirt@us.ibm.com to track the vulnerability - currently rated as HIGH severity.

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

Affected Vendor/Software: **IBM** - **WebSphere Application Server ND** 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 ND is vulnerable to Directory Traversal vulnerability (CVE-2021-20517)	www.ibm.com text/html	CONFIRM www.ibm.com/support/pages/node/6456955
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF ibm-websphere-cve202120517-dir-traversal (198435)

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

Exploit/POC from Github

PoC for exploiting CVE-2021-20517

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ibm	Websphere Application Server Nd	All	All	All	All

cpe:2.3:a:ibm:websphere_application_server_nd:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@knaepp	PH35098:Directory Traversal vulnerability in WebSphere Application Server ND (CVE-2021-20517 CVSS 6.4) tinyurl.com/yjhwwzqc	2021-05-27 15:45:03
@CVEreport	CVE-2021-20517 : #IBM WebSphere Application Server Network Deployment 8.5 and 9.0 could allow a remote authenticate… twitter.com/i/web/status/1…	2021-06-07 14:08:09
/r/netcve	CVE-2021-20517	2021-06-07 14:41:25

← Previous ID

Next ID→

© CVE.report 2023 | |
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 registred 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