

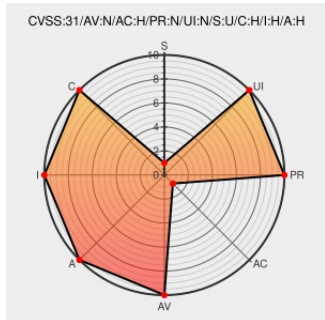


CVE-2021-26912

Published on: 02/08/2021 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:29:02 PM UTC

CVE-2021-26912

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

Certain versions of [Netmotion Mobility](#) from [Netmotionsoftware](#) contain the following vulnerability:

NetMotion Mobility before 11.73 and 12.x before 12.02 allows unauthenticated remote attackers to execute arbitrary code as SYSTEM because of Java deserialization in SupportRpcServlet.

CVE-2021-26912 has been assigned by [M](#) [cve@mitre.org](#) to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **8.1 - HIGH**

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

CVSS2 Score: **9.3 - HIGH**

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

CVE References

Description	Tags	Link
8 February 2021 Update: Security vulnerabilities in Mobility web servers prior to 11.73 / 12.02 NetMotion Software	Vendor Advisory www.netmotionsoftware.com text/html	N MISC www.netmotionsoftware.com/security-advisories/security-vulnerability-in-mobility-web-server-november-19-2020

 MISC ssd-disclosure.com/?p=4676

 [MISC ssd-disclosure.com/ssd-advisory-netmotion-mobility-server-multiple-deserialization-of-untrusted-data-lead-to-rce/](https://misc.ssd-disclosure.com/ssd-advisory-netmotion-mobility-server-multiple-deserialization-of-untrusted-data-lead-to-rce/)

There are currently no QIDs associated with this CVE

Type	Vendor	Product	Version	Update	Edition	Language
Application	Netmotionsoftware	Netmotion Mobility	All	All	All	All
Application	Netmotionsoftware	Netmotion Mobility	All	All	All	All

```
cpe:2.3:a:netmotionsoftware:netmotion_mobility:*****:*.:
```

```
cpe:2.3:a:netmotionsoftware:netmotion_mobility:*****:*.:
```

Next ID→

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