



CVE-2021-20446

Published on: 02/18/2021 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:29:00 PM UTC

CVE-2021-20446

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

Certain versions of [Maximo For Civil Infrastructure](#) from [ibm](#) contain the following vulnerability:

IBM Maximo for Civil Infrastructure 7.6.2 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 196622.

CVE-2021-20446 has been assigned by [psirt@us.ibm.com](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [IBM](#) - **Maximo for Civil Infrastructure** version **7.6.2**

CVSS3 Score: **5.4 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
CHANGED	LOW	LOW	NONE

CVSS2 Score: **3.5 - LOW**

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

CVE References

Description	Tags	Link
IBM X-Force Exchange	VDB Entry	XF ibm-maximo-cve202120446-xss

Vendor Advisory (196622)
exchange.xforce.ibmcloud.com
text/html

Security Bulletin: IBM Maximo Data Loader (maxloader) shipped with IBM Maximo for Civil Infrastructure is vulnerable to cross-site scripting and missing or insecure "X-XSS-Protection" header

Patch
Vendor Advisory
www.ibm.com
text/html

 CONFIRM
www.ibm.com/support/pages/node/6415893

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	Maximo For Civil Infrastructure	7.6.2	All	All	All
Application	Ibm	Maximo For Civil Infrastructure	7.6.2	All	All	All
Operating System	Linux	Linux Kernel	-	All	All	All
Operating System	Linux	Linux Kernel	-	All	All	All
Operating System	Linux	Linux Kernel	-	All	All	All
Operating System	Microsoft	Windows	-	All	All	All
Operating System	Microsoft	Windows	-	All	All	All
Operating System	Microsoft	Windows	-	All	All	All

cpe:2.3:a:ibm:maximo_for_civil_infrastructure:7.6.2:*:*:*:*:*:

cpe:2.3:a:ibm:maximo_for_civil_infrastructure:7.6.2:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:

cpe:2.3:o:microsoft:windows:*:*:*:*:*:

cpe:2.3:o:microsoft:windows:*:*:*:*:*:

cpe:2.3:o:microsoft:windows:*:*:*:*:*:

No vendor comments have been submitted for this CVE

© [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 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](#)