



CVE-2021-29854

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2021-29854
State	PUBLIC
Assigner	psirt@us.ibm.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-05-03 19:15:00 UTC
Updated	2022-05-11 12:35:00 UTC
Description	IBM Maximo Asset Management 7.6.1.1 and 7.6.1.2 is vulnerable to HTTP header injection, caused by improper validation

Risk And Classification

Problem Types: CWE-116

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	ibm	Maximo Application Suite	8.7	All	All	All
Application	ibm	Maximo Asset Management	7.6.1.1	All	All	All
Application	ibm	Maximo Asset Management	7.6.1.2	All	All	All

References

Reference
IBM X-Force Exchange
Security Bulletin: IBM Maximo Asset Management and the IBM Maximo Manage application in IBM Maximo Application Suite are vulnerable to
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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](#)