



CVE-2020-5014

Published on: 03/08/2021 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:03 PM UTC

CVE-2020-5014

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

Certain versions of [Datapower Gateway](#) from [Ibm](#) contain the following vulnerability:

IBM DataPower Gateway V10 and V2018 could allow a local attacker with administrative privileges to execute arbitrary code on the system using a server-side request forgery attack. IBM X-Force ID: 193247.

CVE-2020-5014 has been assigned by [psirt@us.ibm.com](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [IBM](#) - **DataPower Gateway** version **2018.4.1.0**

Affected Vendor/Software: [IBM](#) - **DataPower Gateway** version **10.0.0.0**

Affected Vendor/Software: [IBM](#) - **DataPower Gateway** version **10.0.1.1**

Affected Vendor/Software: [IBM](#) - **DataPower Gateway** version **2018.4.1.14**

CVSS3 Score: **6.7 - MEDIUM**

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

CVSS2 Score: **4.6 - MEDIUM**

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Security Bulletin: IBM DataPower Gateway vulnerable to an RCE attack (CVE-2020-5014)	Patch Vendor Advisory www.ibm.com text/html	 CONFIRM www.ibm.com/support/pages/node/6426789
IBM X-Force Exchange	VDB Entry Vendor Advisory exchange.xforce.ibmcloud.com text/html	 XF ibm-datapower-cve20205014-ssrf (193247)

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

A POC for IBM Datapower Authenticated Redis RCE Exploit abusing the Test Message Function (CVE-2020-5014)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	ibm	Datapower Gateway	All	All	All	All
Application	ibm	Datapower Gateway	All	All	All	All
cpe:2.3:a:ibm:datapower_gateway:*****:*						
cpe:2.3:a:ibm:datapower_gateway:*****:*						

No vendor comments have been submitted for this CVE

[← 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 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](#)