

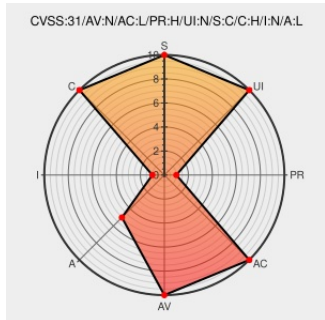


CVE-2020-4509

Published on: 06/04/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:22 PM UTC

CVE-2020-4509

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

Certain versions of [Qradar Security Information And Event Manager](#) from [Ibm](#) contain the following vulnerability:

IBM QRadar SIEM 7.3 and 7.4 is vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 182364.

CVE-2020-4509 has been assigned by [psirt@us.ibm.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [IBM](#) - **QRadar SIEM** version **7.3**

Affected Vendor/Software: [IBM](#) - **QRadar SIEM** version **7.4**

CVSS3 Score: **7.6 - HIGH**

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

CVSS2 Score: **5.5 - MEDIUM**

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

CVE References

Description	Tags	Link
-------------	------	------

Security Bulletin: IBM QHadar is vulnerable to an XML External Entity Injection (XXE) attack (CVE-2020-4509)

Vendor Advisory

www.ibm.com

text/html

CONFIRM

www.ibm.com/support/pages/node/6220154

IBM X-Force Exchange

VDB Entry

Vendor Advisory

exchange.xforce.ibmcloud.com

text/html

XF ibm-gradar-cve20204509-xxe (182364)

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	Qradar Security Information And Event Manager	7.3.0	All	All	All
Application	IBM	Qradar Security Information And Event Manager	7.4.0	All	All	All
Application	IBM	Qradar Security Information And Event Manager	7.3.0	All	All	All
Application	IBM	Qradar Security Information And Event Manager	7.4.0	All	All	All
Operating System	Linux	Linux Kernel	-	All	All	All
Operating System	Linux	Linux Kernel	-	All	All	All
cpe:2.3:a:ibm:qradar_security_information_and_event_manager:7.3.0:*****:						
cpe:2.3:a:ibm:qradar_security_information_and_event_manager:7.4.0:*****:						
cpe:2.3:a:ibm:qradar_security_information_and_event_manager:7.3.0:*****:						
cpe:2.3:a:ibm:qradar_security_information_and_event_manager:7.4.0:*****:						
cpe:2.3:o:linux:linux_kernel:*****:						
cpe:2.3:o:linux:linux_kernel:*****:						

No vendor comments have been submitted for this CVE

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](#)