

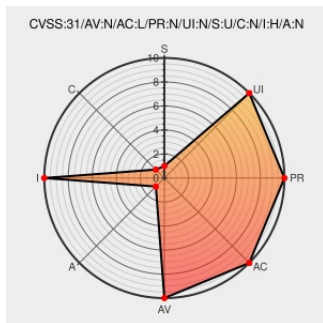


CVE-2019-4545

Published on: 10/08/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:34 PM UTC

CVE-2019-4545

[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 when configured to use Active Directory Authentication may be susceptible to spoofing attacks. IBM X-Force ID: 165877.

CVE-2019-4545 has been assigned by [psirt@us.ibm.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [IBM](#) - **QRadar SIEM** version **7.3.0**

Affected Vendor/Software: [IBM](#) - **QRadar SIEM** version **7.3.3.Patch.4**

Affected Vendor/Software: [IBM](#) - **QRadar SIEM** version **7.4.0**

Affected Vendor/Software: [IBM](#) - **QRadar SIEM** version **7.4.1**

CVSS3 Score: **7.5 - HIGH**

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

CVSS2 Score: **4.3 - MEDIUM**

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

CVE References

Description	Tags	Link
Security Bulletin: IBM QRadar SIEM is vulnerable to KDC Spoofing (CVE-2019-4545)	Patch Vendor Advisory www.ibm.com text/html	 CONFIRM www.ibm.com/support/pages/node/6344077
IBM X-Force Exchange	VDB Entry Vendor Advisory exchange.xforce.ibmcloud.com text/html	 XF ibm-qradar-cve20194545-spoofing (165877)

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	7.3.3	p1	All	All
Application	IBM	Qradar Security Information And Event Manager	7.3.3	p2	All	All
Application	IBM	Qradar Security Information And Event Manager	7.3.3	p3	All	All
Application	IBM	Qradar Security Information And Event Manager	7.3.3	p4	All	All
Application	IBM	Qradar Security Information And Event Manager	7.3.3	p1	All	All
Application	IBM	Qradar Security Information And Event Manager	7.3.3	p2	All	All
Application	IBM	Qradar Security Information And Event Manager	7.3.3	p3	All	All
Application	IBM	Qradar Security Information And Event Manager	7.3.3	p4	All	All
Application	IBM	Qradar Security Information And Event Manager	All	All	All	All
Application	IBM	Qradar Security Information And Event Manager	All	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:7.3.3:p1:*****:
cpe:2.3:a:ibm:qradar_security_information_and_event_manager:7.3.3:p2:*****:
cpe:2.3:a:ibm:qradar_security_information_and_event_manager:7.3.3:p3:*****:
cpe:2.3:a:ibm:qradar_security_information_and_event_manager:7.3.3:p4:*****:
cpe:2.3:a:ibm:qradar_security_information_and_event_manager:7.3.3:p1:*****:
cpe:2.3:a:ibm:qradar_security_information_and_event_manager:7.3.3:p2:*****:

cpe:2.3:a:ibm:qradar_security_information_and_event_manager:7.3.3:p3:~::~~::~~::
cpe:2.3:a:ibm:qradar_security_information_and_event_manager:7.3.3:p4:~::~~::~~::
cpe:2.3:a:ibm:qradar_security_information_and_event_manager::~::~~::~~::
cpe:2.3:a:ibm:qradar_security_information_and_event_manager::~::~general_availability::~::
cpe:2.3:o:linux:linux_kernel::~::~~::~~::
cpe:2.3:o:linux:linux_kernel::~::~~::~~::

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)