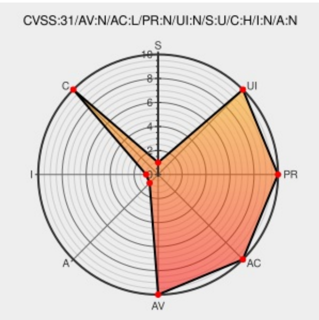
CVE-2020-4269

Published on: 04/15/2020 12:00:00 AM UTC

Last Modified on: 06/29/2022 09:20:00 PM UTC

CVE-2020-4269

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 7.3.0 to 7.3.3 Patch 2 contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data. IBM X-ForceID: 175845.

CVE-2020-4269 has been assigned by psirt@us.ibm.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **IBM** - **Qradar** version **7.3.3.Patch2**

Affected Vendor/Software: **IBM** - **QRadar** version **7.3.0**

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	HIGH	NONE	NONE

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link

QRadar Community Edition 7.3.1.6 Default Credentials ≈ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/157328/QRadar-Community-Edition-7.3.1.6-Default-Credentials.html
Full Disclosure: Unauthorized access to QRadar configuration sets via default password	seclists.org text/html	FULLDISC 20200421 Unauthorized access to QRadar configuration sets via default password
IBM X-Force Exchange	VDB Entry Vendor Advisory exchange.xforce.ibmcloud.com text/html	XF ibm-qradar-cve20204269-info-disc (175845)
Security Bulletin: IBM QRadar SIEM contains hard-coded credentials (CVE-2020-4269)	Vendor Advisory www.ibm.com text/html	CONFIRM www.ibm.com/support/pages/node/6189711

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	All	All	All	All
Application	Ibm	Qradar Security Information And Event Manager	7.3.3	-	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	All	All	All	All
Application	Ibm	Qradar Security Information And Event Manager	7.3.3	-	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
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:*:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:qradar_security_information_and_event_manager:7.3.3:-:*:*:*:*:*:*:

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:*:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:qradar_security_information_and_event_manager:7.3.3:-:*:*:*:*:*:*:

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:o:linux:linux_kernel:-:*:*:*:*:*:*:

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

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@RemotelyAlerts	Severity: ?? | IBM QRadar 7.3.0 to 7.3.3 Patch 2 contai... | CVE-2020-4269 | Link for more: alerts.remotelyrmm.com/CVE-2020-4269	2022-06-29 22:30:17