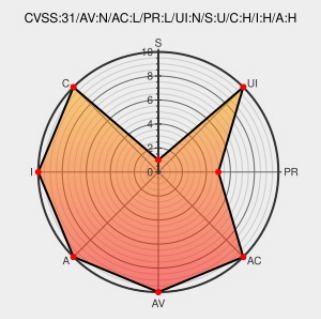
CVE-2020-4280

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

Last Modified on: 06/29/2022 09:14:00 PM UTC

CVE-2020-4280

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 could allow a remote attacker to execute arbitrary commands on the system, caused by insecure deserialization of user-supplied content by the Java deserialization function. By sending a malicious serialized Java object, an attacker could exploit this vulnerability to execute arbitrary commands on the system. IBM X-Force ID: 176140.

CVE-2020-4280 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: 8.8 - HIGH

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

CVSS2 Score: 9 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**

COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Security Bulletin: IBM QRadar SIEM is vulnerable to deserialization of untrusted data	Patch Vendor Advisory www.ibm.com text/html	CONFIRM www.ibm.com/support/pages/node/6344079
QRadar RemoteJavaScript Deserialization ≈ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/159589/QRadar-RemoteJavaScript-Deserialization.html
IBM X-Force Exchange	VDB Entry Vendor Advisory exchange.xforce.ibmcloud.com text/html	XF ibm-qradar-cve20204280-code-exec (176140)
Full Disclosure: Java deserialization vulnerability in QRadar RemoteJavaScript Servlet	seclists.org text/html	FULLDISC 20201016 Java deserialization vulnerability in QRadar RemoteJavaScript Servlet

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: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

Social Mentions

Source	Title	Posted (UTC)
@RemotelyAlerts	Severity: ??? | IBM QRadar SIEM 7.3 and 7.4 could allow ... | CVE-2020-4280 | Link for more: alerts.remotelyrmm.com/CVE-2020-4280	2022-06-29 22:32:05
@ipssignatures	It's new to me that CheckPoint has a protection/signature/rule for the vulnerability CVE-2020-4280.… twitter.com/i/web/status/1…	2022-07-26 14:02:01
@ipssignatures	I know 3 other IPSs that have protections/signatures/rules for the vulnerability CVE-2020-4280. ipssignatures.appspot.com/?cve=CVE-2020-… #Sutllf67pilduo	2022-07-26 14:02:01

← Previous ID

Next ID→