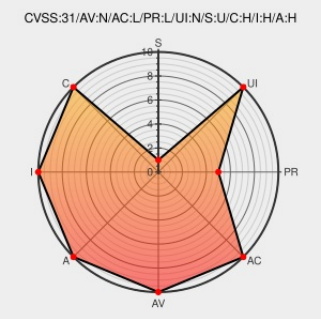
CVE-2020-4272

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

Last Modified on: 04/18/2022 03:15:00 PM UTC

CVE-2020-4272

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 could allow a remote attacker to include arbitrary files. A remote attacker could send a specially-crafted request specify a malicious file from a remote system, which could allow the attacker to execute arbitrary code on the vulnerable server. IBM X-ForceID: 175898.

CVE-2020-4272 has been assigned by psirt@us.ibm.com to track the vulnerability - currently rated as HIGH severity.

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

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

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: 6.5 - MEDIUM

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

CVE References

Description	Tags	Link

Description	Tags	Link
QRadar Community Edition 7.3.1.6 Arbitrary Object Instantiation ≈ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/157337/QRadar-Community-Edition-7.3.1.6-Arbitrary-Object-Instantiation.html
IBM X-Force Exchange	VDB Entry Vendor Advisory exchange.xforce.ibmcloud.com text/html	XF ibm-qradar-cve20204272-file-upload (175898)
Full Disclosure: Arbitrary class instantiation & local file inclusion vulnerability in QRadar Forensics web application	seclists.org text/html	FULLDISC 20200421 Arbitrary class instantiation & local file inclusion vulnerability in QRadar Forensics web application
Security Bulletin: IBM QRadar SIEM is vulnerable to instantiation of arbitrary objects (CVE-2020-4272)	Vendor Advisory www.ibm.com text/html	CONFIRM www.ibm.com/support/pages/node/6189645

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 could ... | CVE-2020-4272 | Link for more: alerts.remotelyrmm.com/CVE-2020-4272	2022-04-18 16:35:54

← Previous ID

Next ID→