

[Full Disclosure](#) mailing list archives[By Date](#) [By Thread](#)

List Archive Search



Local privilege escalation in QRadar due to run-result-reader.sh insecure file permissions

From: "Securify B.V. via Fulldisclosure" <fulldisclosure () seclists.org>

Date: Mon, 20 Apr 2020 12:29:23 +0200

Local privilege escalation in QRadar due to run-result-reader.sh
insecure file permissions

Yorick Koster, September 2019

Abstract

It was found that the nobody user is owner of the run-result-reader.sh script. This script is executed by the root user's crontab. Due to this it is possible for any process running as nobody to add commands to this script that will be executed with root privileges. In combination with a code execution vulnerability in QRadar's web application, this can be used for attacker's to gain full control of the QRadar system.

See also

CVE-2020-4270 [2]
6189657 [3] - IBM QRadar SIEM is vulnerable to privilege escalation (CVE-2020-4270)

Tested versions

This issue was successfully verified on QRadar Community Edition [4] version 7.3.1.6 (7.3.1 Build 20180723171558).

Fix

IBM has released the following versions of QRadar in which this issue has been resolved:

- QRadar / QRM / QVM / QNI 7.4.0 GA [5] (SFS)
- QRadar / QRM / QVM / QRIF / QNI 7.3.3 Patch 3 [6] (SFS)
- QRadar / QRM / QVM / QRIF / QNI 7.3.2 Patch 7 [7] (SFS)
- QRadar Incident Forensics 7.4.0 [8] (ISO)
- QRadar Incident Forensics 7.4.0 [9] (SFS)

Introduction

QRadar [10] is IBM's enterprise SIEM [11] solution. A free version of QRadar is available that is known as QRadar Community Edition [4]. This version is limited to 50 events per second and 5,000 network flows a minute, supports apps, but is based on a smaller footprint for non-enterprise use.

A local privilege escalation vulnerability was found in QRadar. This vulnerability is possible because the script located at /opt/qvm/iem/bin/run-result-reader.sh is configured with weak file permissions. The owner of the script is set to the nobody user, which is a low privileged system account used by various services - including QRadar's web application.

The script is also started by the root user's crontab. This means that if an attacker manages to gain access to the QRadar system as the nobody user, it would be possible to escalate privileges to root. This is for example possible by exploiting a code execution vulnerability in QRadar's web application.

Details

The crontab of the root user contains various entries to run commands on different moments. One of these entries will run the run-result-reader.sh script every 20 minutes:

```
# crontab -l
```

```
[...]
```

```
# Update the Endpoint Manager Fixlet Action Results
```

```
*/20 * * * * /opt/qvm/iem/bin/run-result-reader.sh > /var/log/iem-cron.log 2>&1
```

This script is owned by the nobody user, meaning that this user fully controls the script and thus fully controls which commands will be executed.

```
# ls -la /opt/qvm/iem/bin/run-result-reader.sh
-rwxr-xr-x 1 nobody nobody 2592 Sep 12 17:40
/opt/qvm/iem/bin/run-result-reader.sh
```

If the (modified) script is run from root's crontab, the commands within the script will be executed with root privileges. Due to this it is possible for the nobody to exploit this issue to gain root privileges and gain full control of the QRadar system.

References

- [1] <https://www.securify.nl/advisory/SPY20200405/local-privilege-escalation-in-qradar-due-to-run-result-reader-sh-insecure-file-permissions.html>
[2] <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-4270>
[3] <https://www.ibm.com/support/pages/node/6189657>
[4] <https://developer.ibm.com/qradar/ce/>
[5] <https://www.ibm.com/support/fixcentral/swg/downloadFixes?parent=IBM%20Security&product=IBM/Other+software/IBM+Security+QRadar+SIEM&release=7.4.0&platform=Linux&function=fixIds&fixIds=7.3.3-QRADAR-QRSIEM-20200409085709&includeRequisites=1&includeSupersedes=0&downloadMethod=http>
[6] <https://www.ibm.com/support/fixcentral/swg/downloadFixes?parent=IBM%20Security&product=IBM/Other+software/IBM+Security+QRadar+SIEM&release=7.3.0&platform=Linux&function=fixIds&fixIds=7.4.0-QRADAR-QRSIEM-20200304205308&includeRequisites=1&includeSupersedes=0&downloadMethod=http>
[7] <https://www.ibm.com/support/fixcentral/swg/downloadFixes?parent=IBM%20Security&product=IBM/Other+software/IBM+Security+QRadar+SIEM&release=7.3.0&platform=Linux&function=fixIds&fixIds=7.3.2-QRADAR-QRSIEM-20200406171249&includeRequisites=1&includeSupersedes=0&downloadMethod=http>
[8] <https://www.ibm.com/support/fixcentral/swg/downloadFixes?parent=IBM%20Security&product=IBM/Other+software/IBM+Security+QRadar+SIEM&release=7.3.0&platform=Linux&function=fixIds&fixIds=7.3.2-QRADAR-QRSIEM-20200406171249&includeRequisites=1&includeSupersedes=0&downloadMethod=http>


[parent=IBM%20Security&product=ibm/Other+software/IBM+Security+QRadar+Incident+Forensics&release=7.4.0&platform=Linux&function=fixId&fixids=7.4.0-QRADAR-OIPFULL&2019.18.0.20200304205308&includeRequisites=1&includeSupersedes=0&downloadMethod=http](#)
[9] [https://www.ibm.com/support/fixcentral/swg/downloadFixes?](https://www.ibm.com/support/fixcentral/swg/downloadFixes?parent=IBM%20Security&product=ibm/Other+software/IBM+Security+QRadar+Incident+Forensics&release=7.4.0&platform=Linux&function=fixId&fixids=7.4.0-QRADAR-OIPSEPS-2019.18.0.20200304205308&includeRequisites=1&includeSupersedes=0&downloadMethod=http)
[parent=IBM%20Security&product=ibm/Other+software/IBM+Security+QRadar+Incident+Forensics&release=7.4.0&platform=Linux&function=fixId&fixids=7.4.0-QRADAR-OIPSEPS-2019.18.0.20200304205308&includeRequisites=1&includeSupersedes=0&downloadMethod=http](#)
[10] <https://www.ibm.com/security/security-intelligence/qradar>
[11] https://en.wikipedia.org/wiki/Security_information_and_event_management





Sent through the Full Disclosure mailing list
<https://nmap.org/mailman/listinfo/fulldisclosure>
Web Archives & RSS: <http://seclists.org/fulldisclosure/>

[↩ By Date ↩](#) [↩ By Thread ↩](#)

Current thread:

Local privilege escalation in QRadar due to run-result-reader.sh insecure file permissions *Security B.V. via Fulldisclosure (Apr 21)*



Nmap Security Scanner	Npcap packet capture	Security Lists	Security Tools	About	 
Ref Guide	User's Guide	Nmap Announce	Vuln scanners	About/Contact	
Install Guide	API docs	Nmap Dev	Password audit	Privacy	 
Docs	Download	Full Disclosure	Web scanners	Advertising	
Download	Npcap OEM	Open Source Security	Wireless	Nmap Public Source License	
Nmap OEM		BreachExchange	Exploitation		