

## QRadar Community Edition 7.3.1.6 Insecure File Permissions

Authored by [Yorick Koster](#), [Security B.V.](#)

Posted Apr 21, 2020

QRadar Community Edition version 7.3.1.6 suffers from a local privilege escalation due to insecure file permissions with run-result-reader.sh.

tags | [exploit](#), [local](#)  
advisories | [CVE-2020-4270](#)

SHA-256 | 715d99b55d854b8fb9614afe2a7874cfe20587ea62fbc0dc00f243f7d7096d49 [Download](#) | [Favorite](#) | [View](#)

### Related Files

#### Share This

Like

Twitter

LinkedIn

Reddit

Digg

StumbleUpon

[Change Mirror](#)[Download](#)

-----  
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.security.nl/advisory/SFY20200405/local-privilege-escalation-in-qradar-due-to-run-result-reader\\_sh-insecure-file-permissions.html](https://www.security.nl/advisory/SFY20200405/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%20product-ibm/Other+software/IBM+Security+QRadar+SIEM&release=7.4.0&platform=Linux&function=QRADAR-QRSIEM-20200304205308&includeRequisites=1&includeSupersedes=0&downloadMethod=http>  
[6] <https://www.ibm.com/support/fixcentral/swg/downloadFixes?parent=IBM%20Security%20product-ibm/Other+software/IBM+Security+QRadar+SIEM&release=7.3.0&platform=Linux&function=QRADAR-QRSIEM-20200409085709&includeRequisites=1&includeSupersedes=0&downloadMethod=http>  
[7] <https://www.ibm.com/support/fixcentral/swg/downloadFixes?parent=IBM%20Security%20product-ibm/Other+software/IBM+Security+QRadar+Incident+Forensics&release=7.4.0&platform=Linux&function=QRADAR-QIFFUL-2019.18.0.20200304205308&includeRequisites=1&includeSupersedes=0&downloadMethod=http>  
[8] <https://www.ibm.com/support/fixcentral/swg/downloadFixes?parent=IBM%20Security%20product-ibm/Other+software/IBM+Security+QRadar+Incident+Forensics&release=7.4.0&platform=Linux&function=QRADAR-QIFFUL-2019.18.0.20200304205308&includeRequisites=1&includeSupersedes=0&downloadMethod=http>  
[9] <https://www.ibm.com/support/fixcentral/swg/downloadFixes?parent=IBM%20Security%20product-ibm/Other+software/IBM+Security+QRadar+Incident+Forensics&release=7.4.0&platform=Linux&function=QRADAR-QIFFUL-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](https://en.wikipedia.org/wiki/Security_information_and_event_management)

### File Archive: December 2022 <

Su	Mo	Tu	We	Th	Fr
Sa					
				1	2
3					
4	5	6	7	8	9
10					
11	12	13	14	15	16
17					
18	19	20	21	22	23
24					
25	26	27	28	29	30
31					

### Top Authors In Last 30 Days

Red Hat 150 files
Ubuntu 68 files
LiquidWorm 23 files
Debian 16 files
malvuln 11 files
nu11security 11 files
Gentoo 9 files
Google Security Research 6 files
Julien Ahrens 4 files
T. Weber 4 files

### File Tags

ActiveX (932)  
Advisory (79,754)  
Arbitrary (15,694)  
BBS (2,859)  
Bypass (1,619)  
CGI (1,018)  
Code Execution (8,926)  
Conference (673)  
Cracker (840)  
CSRF (3,290)  
DoS (22,602)  
Encryption (2,349)  
Exploit (50,359)  
File Inclusion (4,165)  
File Upload (946)  
Firewall (821)  
Info Disclosure (2,660)  
Intrusion Detection (867)  
Java (2,899)  
JavaScript (821)  
Kernel (6,291)  
Local (14,201)  
Magazine (586)  
Overflow (12,419)  
Perl (1,418)  
PHP (5,093)  
Proof of Concept (2,291)  
Protocol (3,435)  
Python (1,467)  
Remote (30,044)  
Root (3,504)  
Ruby (594)  
Scanner (1,631)  
Security Tool (7,777)  
Shell (3,103)  
Shellcode (1,204)  
Sniffer (886)

### File Archives

December 2022  
November 2022  
October 2022  
September 2022  
August 2022  
July 2022  
June 2022  
May 2022  
April 2022  
March 2022  
February 2022  
January 2022  
Older

### Systems

AIX (426)  
Apple (1,926)  
BSD (370)  
CentOS (55)  
Cisco (1,917)  
Debian (6,634)  
Fedora (1,600)  
FreeBSD (1,242)  
Gentoo (4,272)  
HPUX (878)  
IOS (330)  
iPhone (108)  
iRIX (220)  
Juniper (67)  
Linux (44,315)  
Mac OS X (684)  
Mandriva (3,105)  
NetBSD (255)  
OpenBSD (479)  
RedHat (12,469)  
Slackware (941)  
Solaris (1,607)

◀

Login or Register to add favorites

▶

- Spoof (2,166)

SQL Injection (16,102)

TCP (2,379)

Trojan (686)

UDP (676)

Virus (662)

Vulnerability (31,136)

Web (9,365)

Whitepaper (3,729)

x86 (946)

XSS (17,494)

Other
- SUSE (1,444)

Ubuntu (8,199)

UNIX (9,159)

UnixWare (185)

Windows (6,511)

Other



© 2022 Packet Storm. All rights reserved.

Site Links


- News by Month
- News Tags
- Files by Month
- File Tags
- File Directory


About Us

- History & Purpose
- Contact Information
- Terms of Service
- Privacy Statement
- Copyright Information

Hosting By

Rokasec

 Follow us on Twitter

 Subscribe to an RSS Feed