Authorization bypass in QRadar Forensics web application

From: "Securify B.V. via Fulldisclosure" <fulldisclosure () seclists org>
Date: Mon, 20 Apr 2020 12:32:58 +0200

```
------------------------------------------------------------------------
Authorization bypass in QRadar Forensics web application
------------------------------------------------------------------------
Yorick Koster, September 2019

------------------------------------------------------------------------
Abstract
------------------------------------------------------------------------
It was found that any authenticated user can access & use the QRadar
Forensics web application, regardless whether they are granted
permission to use the Forensics application. This bypass only requires
that the user manually sets a cookie named QRIF with the same value as
the user's session cookie.

------------------------------------------------------------------------
See also
------------------------------------------------------------------------
CVE-2020-4274 [2]
6189705 [3] - IBM QRadar SIEM is vulenrable to Authorization bypass
(CVE-2020-4274)

------------------------------------------------------------------------
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 QRader 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.

The QRadar Forensics web application is normally only accessible for
users that are granted permission to use this application. A centralized
control that checks if the user has permission is implemented in an
include file that is included in most pages. This check can be bypassed
by sending a QRIF cookie to the application. If this cookie is present
and has the same value as the SEC cookie, the permission check is not
performed. Consequently, any authenticated user can access & use the
Forensics web application.

------------------------------------------------------------------------
Details
------------------------------------------------------------------------
Most PHP pages of the Forensics application (directly or indirectly)
include the PHP file includes/functions.inc.php. A number of checks have
been implemented in this file, including a check to validate the user's
session, a check to detect Cross-Site Request Forgery attacks, and a
permission check to validate if the user has permission to use the
Forensics application. This last check is implemented in the LoginUser()
method of the QRadarHelper class.

/opt/ibm/forensics/html/DejaVu/qradar_helper.php:
public function LoginUser($sessionToken, &$errorInfo)
{
        global $s, $u, $QR_HELPER_CODES;
[...]
        $qrUserHasForensicsAccess = $this->GetQRuserHasForensics($qr_user_info['username']);

The call to LoginUser() is executed from the LoginCurrentUser() method,
which in turn is called form the functions.inc.php include file.

/opt/ibm/forensics/html/includes/functions.inc.php:
require_once('DejaVu/qradar_helper.php');

if (!isset($qrh))
{
        $qrh = new QRadarHelper();

[...]
        $errorMessage = "";
        $userLoggedIn = $qrh->LoginCurrentUser(true, $errorMessage);

Before the call to LoginUser() is made, the LoginCurrentUser() method
first checks if it has received a QRIF cookie. If the cookie is present
and it has the same value of the SEC cookie (the session cookie) the
call to LoginUser() is not made. Not calling LoginUser() also means that
no check is made to validate of the user has permission to use the
Forensics application.

/opt/ibm/forensics/html/DejaVu/qradar_helper.php:
public function LoginCurrentUser ($remember, &$errorInfo)
{
[...]
        if(isset($_COOKIE['QRIF']))
        {
                //if the current cookie is the same as the session token that means user hasn't changed
                //just update the expiry time
                if ($_COOKIE['QRIF'] === $this->session_token)
                {
                        //if cookie is available that means it hasn't expired yet so we need to update it's expiry
time
                        //if cookie expiry time is set to 0 (expire with browser) then we don't update it
                        if($cookieExpiryTime > 0)
                        {
                                unset($_COOKIE['QRIF']);
                                setcookie("QRIF", $this->session_token, $cookieExpiryTime, "/", $_SERVER['HTTP_HOST'],
true, true);
                        }
                        return true;
                }
                else
                {
                        unset($_COOKIE['QRIF']);
                }
        }
        //first time through, login the user and set the cookie
        $loginSuccess = $this->LoginUser($this->session_token, $errorInfo);
        if ($loginSuccess && $remember) {
                setcookie("QRIF", $this->session_token, $cookieExpiryTime, "/", $_SERVER['HTTP_HOST'], true, true);
        }
        return $loginSuccess;
}
```

By manually setting a QRIF cookie, it is possible for an authenticated user without Forensics permissions to access and use most parts of the Forensics application. It should be noted that after passing the LoginCurrentUser() method, another method is called that checks if the user's session is still valid. Meaning that this bypass effectively only bypasses the Forensics permission check.

References
----

[1] https://www.securify.nl/advisory/SFY20200408/authorization-bypass-in-qradar-forensics-web-application.html
[2] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-4274
[3] https://www.ibm.com/support/pages/node/6189705
[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=fixId&fixids=7.4.0-QRADAR-QRSIEM-20200304205308&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=fixId&fixids=7.3.3-QRADAR-QRSIEM-20200409085709&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=fixId&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+Incident+Forensics&release=7.4.0&platform=Linux&function=fixId&fixids=7.4.0-QRADAR-QIFFULL-2019.18.0.20200304205308&includeRequisites=1&includeSupersedes=0&downloadMethod=http
[9]
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-QIFSFS-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

By Date By Thread

Current thread:

- **Authorization bypass in QRadar Forensics web application** *Securify B.V. via Fulldisclosure (Apr 21)*

Site Search

Nmap Security Scanner
Ref Guide
Install Guide
Docs
Download
Nmap OEM

Npcap packet capture
User's Guide
API docs
Download
Npcap OEM

Security Lists
Nmap Announce
Nmap Dev
Full Disclosure
Open Source Security
BreachExchange

Security Tools
Vuln scanners
Password audit
Web scanners
Wireless
Exploitation

About
About/Contact
Privacy
Advertising
Nmap Public Source License