

QRadar Community Edition 7.3.1.6 Authorization Bypass

Authored by Yorick Koster, Security B.V.

Posted Apr 21, 2020

QRadar Community Edition version 7.3.1.6 suffers from an authorization bypass vulnerability.

tags | exploit, bypass

advisories | CVE-2020-4274

SHA-256 | eaeefd76762cac1aef9a9ba909eae0231fa2f6033f281a8d3c45881d26db41f86 Download | Favorite | View

Related Files

Share This

Like

Twitter

LinkedIn

Reddit

Digg

StumbleUpon

Change Mirror

Download

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 vulnerable 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 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.

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($sessionToken, &$amp;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 from the functions.inc.php include file.

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

```
if (!isset($qth))
{
    $qth = new QRadarHelper();

    [...]
    $errorMessage = "";
    $userLoggedIn = $qth->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 if the user has permission to use the Forensics application.

```
/opt/ibm/forensics/html/DejaVu/qradar_helper.php:
public function LoginCurrentUser($remember, &$amp;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) {
```

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)

```
        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=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=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=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=QRADAR-QIFSFS-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=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
```

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	



Login or Register to add favorites





© 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