QRadar Community Edition 7.3.1.6 PHP Object Injection

Authored by Yorick Koster, Securify B.V.

Posted Apr 21, 2020

QRadar Community Edition version 7.3.1.6 suffers from a php object injection vulnerability.

tags | exploit, php
advisories | CVE-2020-4271
SHA-256 | f3ead7ab6cd9ff80673ed0eb62aee04ea3cf3ec0b0842fbda2123d7595ae9847

Download | Favorite | View

Related Files

Share This

Like Twee LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
------------------------------------------------------------------------
PHP object injection vulnerability in QRadar Forensics web application
------------------------------------------------------------------------
Yorick Koster, September 2019

------------------------------------------------------------------------
Abstract
------------------------------------------------------------------------
A PHP object injection vulnerability was found in the QRadar Forensics
web application. The vulnerability can be triggered via a specially
crafted cookie and can be used by an authenticated attacker to execute
arbitrary commands. The commands will be executed with the privileges of
the Apache system user.

------------------------------------------------------------------------
See also
------------------------------------------------------------------------
CVE-2020-4271 [2]
6189651 [3] - IBM QRadar SIEM is vulnerable to PHP object injection
(CVE-2020-4271)

------------------------------------------------------------------------
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.

A PHP object injection vulnerability was found in the QRadar Forensics
web application. The vulnerability exists in the DataSetModel class and
can be triggered via a specially crafted cookie. By exploiting this
issue it is possible for authenticated users to instantiate arbitrary
PHP objects. It has been confirmed that a POP chain exists that can be
used to execute arbitrary commands. The commands will be executed with
the privileges of the Apache system user (generally the nobody user).

------------------------------------------------------------------------
Details
------------------------------------------------------------------------
The Forensics web application contains functionally to save graph data
in cookies. When a graph is viewed that was previously saved, the data
will be restored from the cookie value(s). Saving and restoring data is
done using PHP object serialization. The serialized data is compressed
and encoded with base64 before it is returned as cookie to the user.
Deserialization of graph cookies is done in the restore() method of the
DataSetModel as is shown in the code fragment below.

/opt/ibm/forensics/html/DejaVu/Reports/DataSetModel.php:
public function restore($dataKeys, $dsize) {
  if ($dsize == 0)
  // No data
    return null;

  $cookieData = '';
  foreach ($dataKeys as $dataKey) {
    if (array_key_exists($dataKey, $_COOKIE)) {
      $cookieData .= $_COOKIE[$dataKey];
      // All done, so delete the data cookie.
      setcookie($dataKey, "", time() - 3600);
    } else {
      error_log("MISSING COOKIE '$dataKey'");
      return null;
    }
  }

  $sz = strlen($cookieData);
  if ($sz != $dsize) {
    error_log("ERROR: Graph data size incorrect: expected $dsize, got $sz");
    return null;
  }

  try {
    $dataset = unserialize(gzuncompress(base64_decode($cookieData)));
    return $dataset;
  } catch (Exception $e) {
    error_log("Error deserializing session data: " . $e->getMessage());
    $dataset = null;
  }
  return null;
}

The restore() method is called in the constructor of various chart
classes, which all inherit from the BaseChart class. These chart classes
are exposed in the /forensics/graphs.php page of the Forensics web
application.

/opt/ibm/forensics/html/DejaVu/Charts.php:
abstract class BaseChart extends ParameterizedObject {
[...]
  public function __construct($params=null) {
[...]

        $dm = empty($dmodel) ? new DataSetModeler(null) : new $dmodel(null);
        if(array_key_exists('sid',$_GET))
            $dm->setSessID($_GET['sid']);

        $dataset = $dm->restore($dataKeys,$dsize);
[...]

It has been confirmed that this vulnerability can be used to execute
arbitrary commands by sending a specially crafted cookie to the affected
web page.
```

Follow us on Twitter

Subscribe to an RSS Feed

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
nu11secur1ty	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	(6,926)
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	(1,690)
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)

```
------------------------------------------------------------------------
References
------------------------------------------------------------------------
[1] https://www.securify.nl/advisory/SFY20200406/php-object-injection-vulnerability-in-qradar-forensics-web-
application.html
[2] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-4271
[3] https://www.ibm.com/support/pages/node/6189651
[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=L
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=L
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
```

Login or Register to add favorites

Spoof (2,166)
SQL Injection (16,102)
TCP (2,379)
Trojan (686)
UDP (876)
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

packet storm

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