QRadar RssFeedItem Server-Side Request Forgery vulnerability

From: "Securify B.V. via Fulldisclosure" <fulldisclosure () seclists org>
Date: Mon, 20 Apr 2020 12:26:32 +0200

```
--------------------------------------------------------------------------
QRadar RssFeedItem Server-Side Request Forgery vulnerability
--------------------------------------------------------------------------
Yorick Koster, September 2019

--------------------------------------------------------------------------
Abstract
--------------------------------------------------------------------------
The RssFeedItem class of the QRadar web application is used to fetch and
parse RSS feeds. No validation is performed on the user-supplied RSS
feed URL. Due to the lack of URL validation (whitelisting), it is
possible for authenticated attackers to execute Server-Side Request
Forgery attacks. Using this issue it is possible to call the Apache Axis
AdminService webservice in order to execute arbitrary code with the
privileges of the Tomcat user.

--------------------------------------------------------------------------
See also
--------------------------------------------------------------------------
CVE-2020-4294 [2]
6189663 [3] - IBM QRadar SIEM is vulnerable to Server-Side Request
Forgery (SSRF) (CVE-2020-4294)

--------------------------------------------------------------------------
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 RssFeedItem class of the QRadar web application is used to fetch and
parse (and cache) RSS feeds. The class is exposed in the JSON-RPC
interface via the qradar.getRssFeedItem method. This method can be
called by any authenticated user, no special privileges are required.
RSS feeds are fetched using the Apache Commons HttpClient class, no
validation is performed on the user-supplied URL. Due to the lack of URL
validation (whitelisting), it is possible for authenticated attackers to
execute Server-Side Request Forgery attacks.

--------------------------------------------------------------------------
Details
--------------------------------------------------------------------------
Authenticated users can trigger the Server-Side Request Forgery
vulnerability by making a JSON-RPC call with the method set to
qradar.getRssFeedItem. This call is mapped to
com.qllabs.qradar.ui.dashboard.RssFeedItem.getRssFeedItem() and takes
one parameter named feedURL. Any valid URL can be passed to this method.

com.qllabs.qradar.ui.dashboard.RssFeedItem:
public class RssFeedItem extends DashboardItem {
[...]

        public static DashboardItem getRssFeedItem(PageContext pageContext, String feedURL) throws Exception {
                sessionContext = RequestUtils.getSessionContext((HttpServletRequest)pageContext.getRequest());
                RssFeedItem cachedItem = (RssFeedItem)feedCache.get(feedURL);
                cachedItem = null;
                if (cachedItem == null || System.currentTimeMillis() - cachedItem.lastUpdateTime >= 600000L) {
                        cachedItem = new RssFeedItem(pageContext, feedURL);
                        feedCache.put(feedURL, cachedItem);
                }

                return cachedItem;
        }

No validation is done on the user-supplied URL, it is directly passed to
HttpClient that will try to make a GET request to this URL. This
behavior allows for Server-Side Request Forgery. The returned HTTP
response is parsed as RSS feed. If the response isn't a valid RSS feed,
an error is returned to the user. Due to this it is not possible to read
the HTTP response, however the GET request is still executed. By abusing
this vulnerability it is possible for an authenticated attacker to make
GET requests to services that are normally not accessible, including
webservices of QRadar that can only be accessed from the local machine.

com.qllabs.qradar.ui.dashboard.RssFeedItem:
public RssFeedItem(PageContext pageContext, String rssURLString) {
        GetMethod getMethod = null;
        Locale locale = LocaleUtil.getLocale((HttpServletRequest)pageContext.getRequest());

        try {
                getMethod = new GetMethod(rssURLString);
                HttpClient client = new HttpClient();
                ISessionContext sessionContext =
RequestUtils.getSessionContext((HttpServletRequest)pageContext.getRequest());
                UIAutoupdateService autoupdateService = UIAutoupdateService.getInstance();
                String proxyHost = autoupdateService.getSetting(sessionContext, "proxy_server");
                String proxtPortString = autoupdateService.getSetting(sessionContext, "proxy_port");
                int proxyPort;

[...]

                try {
                        proxyPort = client.executeMethod(getMethod);
```

```
                this.log.debug("Proxy request successful.");
        } catch (Exception var29) {
                this.log.warn("Proxy request failed. Falling back to default HTTP request.");
                if (StringUtils.isNotEmpty(client.getHostConfiguration().getProxyHost())) {
                        client = new HttpClient();
                        proxyPort = client.executeMethod(getMethod);
                }
        }
```

The QRadar web application is deployed with Apache Axis [12] version 1.2
to expose a number of SOAP services. The AdminService webservice is
enabled, which allows deploying and undeploying of webservices. The
enableRemoteAdmin option is set to false, meaning that the webservice
can only be called from localhost. By abusing the Server-Side Request
Forgery vulnerability it is possible to call the AdminService webservice
and execute arbitrary code.

References

---

[1] https://www.securify.nl/advisory/SFY20200402/qradar-rssfeeditem-server-side-request-forgery-vulnerability.html
[2] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-4294
[3] https://www.ibm.com/support/pages/node/6189663
[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&f
unction=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&f
unction=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
[12] http://axis.apache.org/

By Date By Thread

Current thread:

QRadar RssFeedItem Server-Side Request Forgery vulnerability ***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