R Advisory Database

RConsortium

Vulnerabilities in R Packages

- Vulnerabilities are typically caused by external library uses
- Lack of open-source alternatives hinders R adoption in companies with tight security protocols
- Security researchers aren’t incentivized to study the R ecosystem when compared to PyPI or other language package repositories
- Some CVEs are tracked through security-tracker.debian.org or through company like snyk, JFrog, and Sonatype but these aren’t accessible or easily updated

OSSF & OSV

- In 2022, Google announced the OSV-Scanner, the Open Source Vulnerability (OSV) schema, and launched the OSV.dev service, the first distributed open source vulnerability database
- The database launched with support for PyPI, npm, and other package repositories
- Last year, we started the r-advisory-database modeled after PyPA's advisory database
  - https://github.com/pypa/advisory-database
  - https://github.com/rconsortium/r-advisory-database

Source: https://security.googleblog.com/2022/12/announcing-osv-scanner-vulnerability.html

Announcing OSV-Scanner: Vulnerability Scanner for Open Source

December 13, 2022

Posted by Rex Pan, software engineer, Google Open Source Security Team

Today, we're launching the OSV-Scanner, a free tool that gives open source developers easy access to vulnerability information relevant to their project.

Last year, we undertook an effort to improve vulnerability triage for developers and consumers of open source software. This involved publishing the Open Source Vulnerability (OSV) schema and launching the OSV.dev service, the first distributed open source vulnerability database. OSV allows all the different open source ecosystems and vulnerability databases to publish and consume information in one simple, precise, and machine readable format.

The OSV-Scanner is the next step in this effort, providing an officially supported frontend to the OSV database that connects a project's list of dependencies with the vulnerabilities that affect them.

R Advisory Database

The R Advisory Database:

- Was accepted onto the osv.dev service https://osv.dev/list?ecosystem=CRAN
- Contains almost a dozen package vulnerabilities
- Continues to grow as vulnerabilities are reported

RSEC-2023-9

Import Source	https://github.com/RConsortium/r-advisory-database/blob/main/vulns/gdata/RSEC-2023-9.yaml
Aliases	CVE-2023-7101
Published	2023-12-28T02:15:00Z
Modified	2024-01-04T16:41:35.876798Z
Details	Bundled Perl script Spreadsheet::ParseExcel version 0.65 is vulnerable to an arbitrary code execution (ACE) vulnerability due to passing unvalidated input from a file into a string-type "eval". Specifically, the issue stems from the evaluation of Number format strings (not to be confused with printf-style format strings) within the Excel parsing logic. Fixed with the depreation of Excel-related functionality from gdata version 3.0.0 -- upgrading advised.
References	https://security-tracker.debian.org/tracker/CVE-2023-7101 https://github.com/r-gregmisc/gdata/issues/14

Affected packages

CRAN
gdata

Package

Name gdata

Affected ranges

Type ECOSYSTEM

Events		
	Introduced	2.16.1
	Fixed	3.0.0

Affected versions

▶ 2.*

Next Steps

While this is great, there's still more needed

- New vulnerabilities and proposed vulnerabilities are accepted on an ad-hoc basis
  - Should we codify community guidelines?
- Without searching or knowing about OSV, it's hard to know it exists
  - How can we make the R Advisory Database more visible?
- Contribution steps are manual and assigning an ID can lead to collisions
  - Ecosystem vulnerabilities need unique IDs and these are currently incremented manually by the vulnerability author?

Thanks