

Dependency vulnerability check in The Nistagram

Golang application

We decided to manually check for dependencies vulnerabilities in The Nistagram Golang application. The decision was made to use the Sonatype OSS Index as a base tool. It is a free catalogue of open source components and scanning tools to help developers identify vulnerabilities, understand risk, and keep their software safe.

Steps for running a dependency vulnerability test

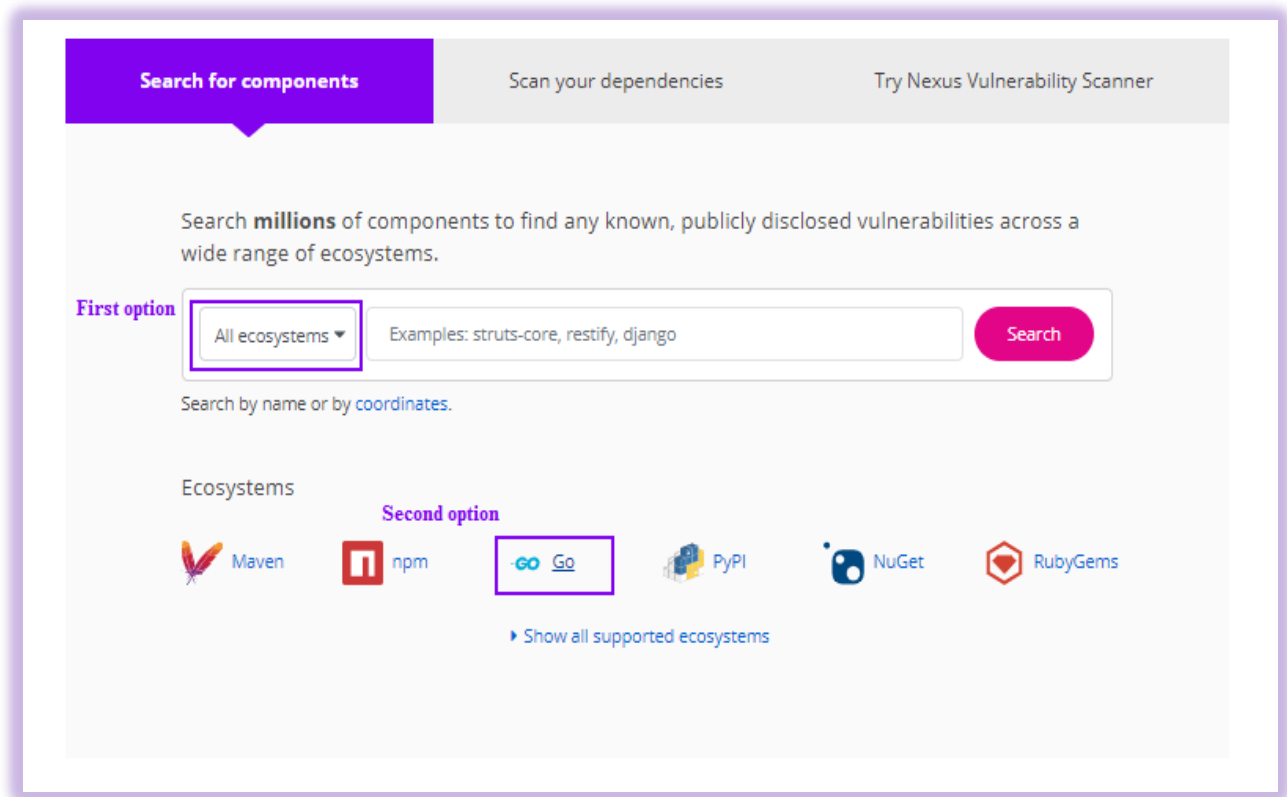
1. The initial step

Although it goes without saying, we will state that the initial step is to go to [The official website of the OSS index](#).



2. Ecosystem selection

Ecosystem selection facilitates the verification and search for dependency vulnerabilities, we can do this in two ways - by selecting an item from the combo box or simply clicking on the icon that represents our ecosystem in which we develop the application.



3. Search vulnerabilities for chosen dependency

The search is very simple, all you have to do is enter the name of the dependency in the input field, and then click on the search button. After that display, you will see the search results, of course, there is a possibility that several other dependencies have the same name in the repository path, pay special attention to find your dependency.


Golang Components

Search Components

Golang

Examples: struts-core, testify, django

Search

ECOSYSTEM	COMPONENT	DESCRIPTION
Golang	google.golang.org/grpc	
Golang	go.etcd.io/etcd	
Golang	golang.org/x/text	
Golang	k8s.io/client-go	
Golang	github.com/golang/protobuf	
Golang	github.com/stretchr/testify	
Golang	github.com/davecgh/go-spew	
Golang	github.com/pkg/errors	
Golang	github.com/google/go-cmp	
Golang	github.com/pmezard/go-difflib	
Golang	google.golang.org/appengine	
Golang	github.com/sirupsen/logrus	
Golang	github.com/aws/aws-sdk-go	
Golang	github.com/golang/mock	
Golang	k8s.io/apimachinery	
Golang	github.com/konsorten/go-windows-terminal-sequences	
 Golang	github.com/gogo/protobuf	
Golang	gopkg.in/src-d/go-git.v4	

Example of positive outcome- dependency has no vulnerabilities

Fortunately, mostly in our dependencies, no vulnerabilities have been detected. We have now chosen, e.g. "gopkg.in/go-playground/validator.v9" dependency that we use to validate the data on the back-end of our application, just to show you one example of a positive outcome.

Component Results

⚠ = has vulnerabilities

Search Components

Golang

validator

Search

ECOSYSTEM	COMPONENT	DESCRIPTION
Golang	gopkg.in/go-playground/validator.v9	
Golang	gopkg.in/go-playground/validator.v8	
Golang	github.com/go-courier/validator	
Golang	github.com/go-dragon/validator	



gopkg.in/go-playground/validator.v9

<https://pkg.go.dev/gopkg.in/go-playground/validator.v9>

Vulnerabilities

No vulnerabilities detected

Example of negative outcome - dependency has vulnerabilities

One dependency we used in our project has a vulnerability. It is this "github.com/dgrijalva /jwt-go" dependency that we used to work with tokens.

 **github.com/dgrijalva/jwt-go**
<https://pkg.go.dev/github.com/dgrijalva/jwt-go>

Vulnerabilities

1  CRITICAL

We will show you how we discovered exactly what that vulnerability is. We used the National Vulnerability Database (NVD), which is the U.S. government repository of standards-based vulnerability management, data represented using the Security Content Automation Protocol (SCAP). NVD includes databases of security checklists, security related software flaws, misconfigurations, product names, and impact metrics. In addition to providing a list of Common Vulnerabilities and Exposures (CVEs), the NVD scores vulnerabilities using the Common Vulnerability Scoring System (CVSS) which is based on a set of equations using metric such as access complexity. Using NVD, we will show you step by step in this example.

1. The First step

The first step is going to the official website of [NVD - Search and Statistics](#).

2. Search Vulnerability

We enter the keyword on the basis of which the search is performed, in our case "github.com/dgrijalva/jwt-go", and then click on the search button.

Information Technology Laboratory

NATIONAL VULNERABILITY DATABASE

NVD

VULNERABILITIES

Search Vulnerability Database

Try a product name, vendor name, CVE name, or an OVAL query.

NOTE: Only vulnerabilities that match ALL keywords will be returned, Linux kernel vulnerabilities are categorized separately from vulnerabilities in specific Linux distributions. Search results will only be returned for data that is populated by NIST or from source of Acceptance Level "Provider".

Search Type
☒ Basic ☐ Advanced

Results Type
☒ Overview ☐ Statistics

Keyword Search

☐ Exact Match

Search Type
☒ All Time ☐ Last 3 Months ☐ Last 3 Years

Contains HyperLinks
☐ US-CERT Technical Alerts
☐ US-CERT Vulnerability Notes
☐ OVAL Queries

Search **Reset**

NIST National Institute of Standards and Technology
U.S. Department of Commerce

Twitter Facebook LinkedIn YouTube RSS Email

3. Vulnerability display

All vulnerabilities for the requested dependency are shown, in our case it is a vulnerability with identification code CVE-2020-26160. Below we will show you how we solved the found vulnerability.

Information Technology Laboratory
NVD

VULNERABILITIES
SEARCH AND STATISTICS

Search Results (Refine Search)

Sort results by:
Publish Date Descending
Sort

Search Parameters:

- Results Type: Overview
- Keyword (text search): github.com/dgrijalva/jwt-go
- Search Type: Search All

There are **1** matching records.
Displaying matches **1** through **1**.

Vuln ID	Summary	CVSS Severity
CVE-2020-26160	<p>jwt-go before 4.0.0-preview1 allows attackers to bypass intended access restrictions in situations with <code>{string}</code> for <code>m["aud"]</code> (which is allowed by the specification). Because the type assertion fails, "" is the value of aud. This is a security problem if the JWT token is presented to a service that lacks its own audience check.</p> <p>Published: сентябрь 30, 2020; 2:15:27 PM -0400</p>	V3.1: 7.5 HIGH V2.0: 5.0 MEDIUM

National Institute of Standards and Technology
U.S. Department of Commerce

Solving vulnerability

We looked for a solution to the found vulnerability and we found it. It was necessary to replace our vulnerable dependency with a new one. So instead of the critical dependency "github.com/dgrijalva/jwt-go", we now use "github.com/form3tech-oss/jwt-go v3.2.3" in The Nistagram application. We found an advice that solves the problem (photo below).

dgrijalva / jwt-go

Watch 151
 Star 9.6k
 Fork 931

<> Code
 Issues 90
 Pull requests 42
 Actions
 Projects
 Wiki
 Security
 Insights

Stable release for CVE-2020-26160 fix #463

Open
 agiammar opened this issue on 12 Apr · 11 comments

agiammar commented on 12 Apr

The CVE-2020-26160 vulnerability is fixed in the preview `v4.0.0-preview1`
Are there any plans to make the fix part of a **stable** release, either V4 or V3?

18

agiammar changed the title ~~Stable release CVE-2020-26160 fix~~ Stable release for CVE-2020-26160 fix on 13 Apr

ewilde commented on 19 Apr

We are maintaining a fixed version of this library <https://github.com/form3tech-oss/jwt-go>

CVE fixed: <https://github.com/form3tech-oss/jwt-go/releases/tag/v3.2.1>

If that is of interest

2

Checked Dependency lists

Dependency name	Vulnerabilities
github.com/fmtlib/fmt	No vulnerabilities detected
github.com/antchfx/xpath v1.1.11	No vulnerabilities detected
github.com/google/uuid	No vulnerabilities detected
github.com/mikespook/gorbac/v2	No vulnerabilities detected
gopkg.in/go-playground/validator.v9	No vulnerabilities detected
github.com/goccy/go-json	No vulnerabilities detected
github.com/json-iterator/go	No vulnerabilities detected
github.com/encoding/json	No vulnerabilities detected
net/http	No vulnerabilities detected

io/ioutil	No vulnerabilities detected
bytes	No vulnerabilities detected
os	No vulnerabilities detected
github.com/tdewolff/strconv	No vulnerabilities detected
github.com/golage/strings	No vulnerabilities detected
github.com/golangplus/time	No vulnerabilities detected
github.com/gorilla/handlers v1.5.1	No vulnerabilities detected
github.com/gorilla/mux v1.8.0	No vulnerabilities detected
github.com/lib/pq v1.10.2	No vulnerabilities detected
gorm.io/driver/postgres v1.1.0	No vulnerabilities detected
gorm.io/gorm v1.21.10	No vulnerabilities detected
gopkg.in/mail.v2	No vulnerabilities detected
github.com/sirupsen/logrus v1.4.2	No vulnerabilities detected
gopkg.in/alexcesaro/quotedprintable.v3	No vulnerabilities detected
gopkg.in/go-playground/assert.v1	No vulnerabilities detected
golang.org/x/crypto v0.0.0-20210513164829-c07d793c2f9a	No vulnerabilities detected
github.com/leodido/go-urn v1.2.1	No vulnerabilities detected
github.com/go-playground/universal-translator v0.17.0	No vulnerabilities detected
github.com/form3tech-oss/jwt-go v3.2.3+incompatible	No vulnerabilities detected

Front-end Node Package Manager (npm) for the JavaScript programming language doesn't show any warnings, i.e. vulnerabilities, so we checked all dependencies and they are safe.

Conclusion

Except for solving the vulnerability that we presented in detail as an example, we had no others. We have achieved satisfactory results, and we have made our Nistagram application have a high security.