Product Security Tools
Friend or Foe

FIRST - PSIRT Technical Colloquium 2020 - March 4-5
About Us

NVIDIA Product Security Tools

Adam Wallis
NVIDIA Product Security Tools Development
awallis@nvidia.com

Jessica Butler
NVIDIA Product Security Tools Development
jessicab@nvidia.com
Intro
Moving the Ball Forward

Foe - Security’s Bad Reputation

Tools Developers Need & WANT

Friend - Delivering Actionable Results

Integrating Security into *Speed of Light* Culture

DEMO 1 - GitHub built-in vulnerability detection

DEMO 2 - pipeline vulnerability detection using *Safety*

DEMO 3 - more advanced configuration using *Clair*

DEMO 4 - integrating external scanning tools like *WhiteSource BOLT*
Developer: ‘Release is scheduled in 3 days. Can you drop everything and help me now?!’

Security: ‘Sure, I’m not doing anything else right now. Usually I just sit around waiting for these types of reactive requests. :) BTW, there will probably be issues and you won’t have time to fix them…’

STOP: Release Checklist

https://gunshowcomic.com/648
## Tools Developers Need

... & WANT!

<table>
<thead>
<tr>
<th>Findings</th>
<th>examples</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Open Source Security</strong></td>
<td>Vulnerable Open Source Software (OSS) Dependencies</td>
</tr>
<tr>
<td>Static Analysis (SAST)</td>
<td>source code defects</td>
</tr>
<tr>
<td>Sensitive Material Detection</td>
<td>detect passwords, profanity, porn</td>
</tr>
<tr>
<td>Dynamic Analysis (DAST)</td>
<td>input/output and configuration issues, unused ports</td>
</tr>
<tr>
<td>Container Scanning</td>
<td>detect vulnerabilities in image</td>
</tr>
</tbody>
</table>
Delivering Actionable Results

Typical developer workflow using pipeline

Integrate into PIPELINE!!
INTEGRATING FOR

**CODE**
- Open Source screening

**BUILD**
- Commit triggered scanning
- Build defined components

**PKG**
- Release tracking

**RELEASE**
- Platform dependencies

**CONFIG**
- Continuous tracking and alerting

**MONITOR**
DEMO 1
GitHub built-in vulnerability detection
We found a potential security vulnerability in one of your dependencies.

Only the owner of this repository can see this message.

requests

GitHub opened this alert 16 hours ago

Bump requests from 2.19.0 to 2.20.0

#1 opened 16 hours ago by dependabot bot

1 requests vulnerability found in requirements.txt 16 hours ago

Remediation

Upgrade requests to version 2.20.0 or later. For example:

requests>=2.20.0

Always verify the validity and compatibility of suggestions with your codebase.

Details

CVE-2018-18074

Vulnerable versions: <= 2.19.1
Patched version: 2.20.0

The Requests package through 2.19.1 before 2018-09-14 for Python sends an HTTP Authorization header to an http URI upon receiving a same-hostname https-to-http redirect, which makes it easier for remote attackers to discover credentials by sniffing the network.
GitHub Vulnerability Detection

How to Enable

Settings

Data services

Use the data from your repository to power these enhanced features.

- **Security alerts**
  Receive alerts when a new vulnerability is found in one of your dependencies.
Pipeline vulnerability detection using Safety
Github + Azure Pipelines + Python Safety

Run security Audit

by pyup.io

REPORT
checked 15 packages, using default DB

<table>
<thead>
<tr>
<th>package</th>
<th>installed</th>
<th>affected</th>
<th>ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>requests</td>
<td>2.19.0</td>
<td>&lt;=2.19.1</td>
<td>36546</td>
</tr>
</tbody>
</table>

The Requests package before 2.19.1 sends an HTTP Authorization header to an http URI upon receiving a same-hostname https-to-http redirect, which makes it easier for remote attackers to discover credentials by sniffing the network.
Add Security Check to Azure Pipeline

Create Azure Pipeline

Add Vulnerability Check
DEMO 3
GitLab container scanning with Clair
Container Scanning with Gitlab

Request to merge `vuln_scan` into `master`

Pipeline #121305332 passed for `6ba274bb on vuln_scan`

No approval required

View eligible approvers

Security scanning detected 42 vulnerabilities for the source branch only

Container scanning detected 42 new vulnerabilities

- Medium: CVE-2018-12886 in gcc-8
- Medium: CVE-2019-13627 in libgCRYPT20
- Medium: CVE-2019-12290 in libidn2
- Low: CVE-2011-3374 in apt
- Low: CVE-2019-18276 in bash

Merge | Delete source branch
Add Container Scanning to Gitlab Pipeline

Create Gitlab Pipeline

Add Security Scanning
Using external scanning tools like WhiteSource BOLT
Automated Issue Creation for Vulnerabilities
CVE-2018-18074 - High Severity Vulnerability

- Vulnerable Library - requests-2.19.0-py2.py3-none-any.whl
- Vulnerability Details
  The Requests package before 2.20.0 for Python sends an HTTP Authorization header to an http URI upon receiving a same-hostname https-to-http redirect, which makes it easier for remote attackers to discover credentials by sniffing the network.
  Publish Date: 2018-10-09
  URL: CVE-2018-18074
- CVSS 3 Score Details (9.8)
- Suggested Fix
  Type: Upgrade version
  Release Date: 2018-10-09
  Fix Resolution: 2.20.0

Check this box to open an automated fix PR
Summary
Shift your security left to move the ball forward!

- **Easily** enable Open Source vulnerability detection using GitHub & dependebot!
  - Github Built In security: [https://github.com/adawalli/first-basic](https://github.com/adawalli/first-basic)

- **Try Out** Safety for Python and **Add** it to an Azure DevOps pipeline

- **Scanning containers** with Clair is as simple as adding a single line!
  - Gitlab + Clair Container Scanning: [https://gitlab.com/adawalli/first-clair](https://gitlab.com/adawalli/first-clair)

- **Transitive dependency vulnerability detection** is delivered with WhiteSource Bolt
  - Github + Whitesource Bolt: [https://github.com/adawalli/first-bolt](https://github.com/adawalli/first-bolt)
Technologies Used In Demo

- Whitesource Bolt
  - https://bolt.whitesourcesoftware.com/
- Whitesource Unified Agent
  - https://www.whitesourcesoftware.com/free-trial-request/
- Python Safety Package
  - https://github.com/pyupio/safety
- Azure Pipelines
- Github Security
  - https://github.com/security
- Gitlab + Clair
  - https://docs.gitlab.com/ee/user/application_security/container_scanning/
THANK YOU!
Comments, Questions, Follow-UP!

We love chatting with other Security Tools developers to knowledge share. Please contact us if you’re interested in learning more or sharing!!

awallis@nvidia.com
jessicab@nvidia.com