



THE DEVELOPER'S CONFERENCE

Trilha – Software Security

Juscélio Reis
Desenvolvedor

Agenda




- Sobre
- Números
- Solargate
- Alex Birsan
- Dependency Track

Sobre o palestrante



THE DEVELOPER'S CONFERENCE

Juscélio Reis

- Pai 
- Geek
- +10 anos de experiencia em desenvolvimento de software.
- Pesquisador



Alguns números



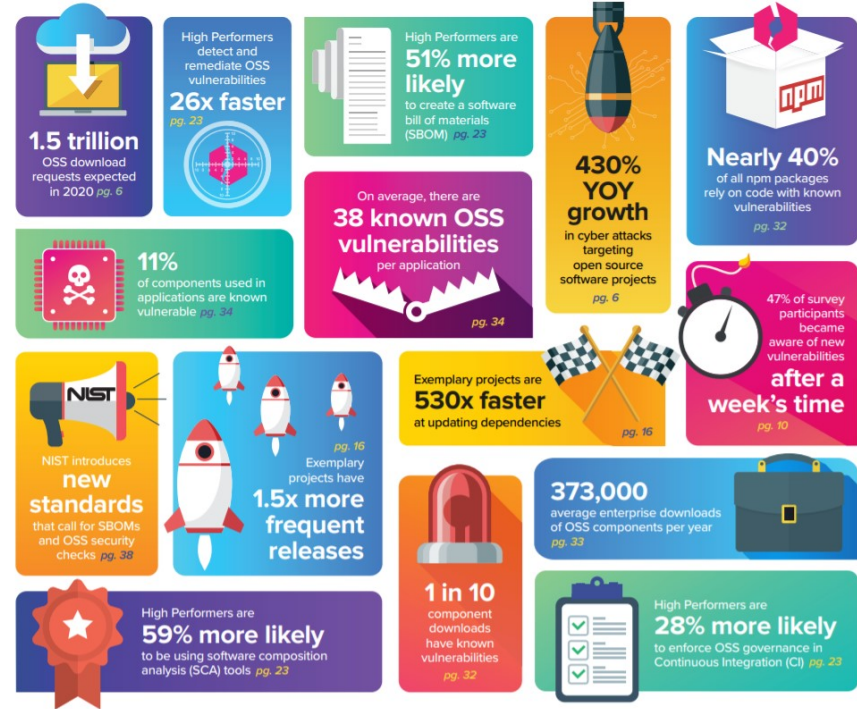
THE
DEVELOPER'S
CONFERENCE

2020 State of the Software Supply Chain

The 6th Annual Report on Global Open Source Software Development

PRESENTED BY
 sonatype

IN PARTNERSHIP WITH
 IT REVOLUTION
 muse dev



SolarGate

NOTÍCIAS | SEGURANÇA E PRIVACIDADE

SolarWinds: ataque foi o “maior e mais sofisticado” que o mundo já viu

Por Rafael Rigues | Editado por André Lucena | © 15 de fevereiro de 2021

Até **18.000 clientes** da **SolarWinds** que usavam o software de monitoramento de rede Orion podem ter sido vítimas do ataque, que ocorreu durante **novê meses ao longo de 2020** antes que fosse detectado.

Os responsáveis

Desde quando a FireEye identificou que estava sendo espionada, **a suspeita é de que seja um grupo diretamente ligado e financiado pelo governo da Rússia**. Mas, a empresa prefere não confirmar essa suspeita por falta de dados de comprovação.

No entanto, pode afirmar que é um grupo **financiado por uma nação**, altamente qualificado, **com habilidades extensas em vários sistemas de tecnologia**, plataformas de software desenvolvidas, **além de vasta estrutura de tecnologia dedicada, capaz de fornecer recursos para uma campanha de longa duração**.



THE
DEVELOPER'S
CONFERENCE

The malicious Orion updates

The software builds for Orion versions 2019.4 HF 5 through 2020.2.1 that were released between March 2020 and June 2020 might have contained a trojanized component. However, FireEye noted in its analysis that each of the attacks required meticulous planning and manual interaction by the attackers.]

The attackers managed to modify an Orion platform plug-in called SolarWinds.Orion.Core.BusinessLayer.dll that is distributed as part of Orion platform updates. The trojanized component is digitally signed and contains a backdoor that communicates with third-party servers controlled by the attackers. FireEye tracks this component as SUNBURST and has released [open-source detection rules](#) for it on GitHub.

Home > Virus & Threats



Microsoft: SolarWinds Hackers Attempted to Access Our Systems Until January 2021

By Eduard Kovacs on February 19, 2021

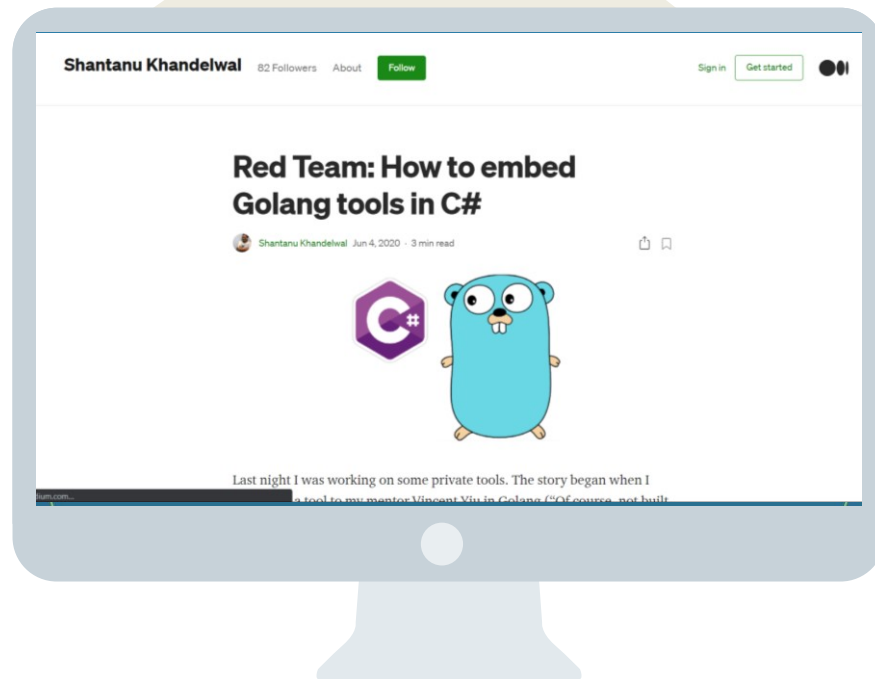
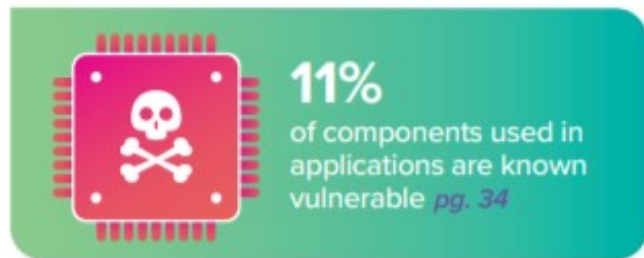


THE
DEVELOPER'S
CONFERENCE

A facilidade...

Não precisa ser patrocinado por uma nação para conseguir elaborar algo que vá prejudicar outras equipes.

Uma pesquisa no google ou seguir as pessoas certas no twitter, já vai conseguir o conhecimento necessário.



Alex Birsan

9 de fevereiro de 2021

Conseguí usar uma forma de colocar componentes comprometidos nos repositórios públicos.

Nuget

Gem

Pip

NPM

Yarn

Maven Central

Gradle

Dependency Confusion: How I Hacked Into Apple, Microsoft and Dozens of Other Companies

The Story of a Novel Supply Chain Attack



Alex Birsan Feb 9 · 11 min read ★



- What happens if malicious code is uploaded to npm under these names?
Is it possible that some of PayPal's internal projects will start defaulting to the new public packages instead of the private ones?

APPLE MICROSOFT TECH

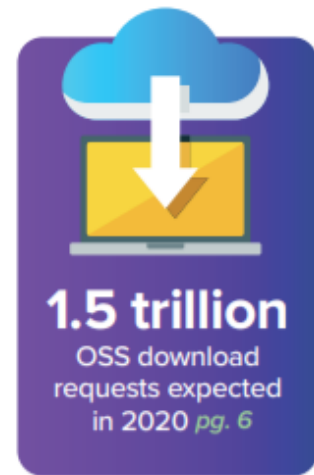
Security researcher finds a way to run code on Apple, PayPal, and Microsoft's systems

The attack is incredibly simple yet fiendishly effective

By Mitchell Clark | Feb 10, 2021, 5:43pm EST



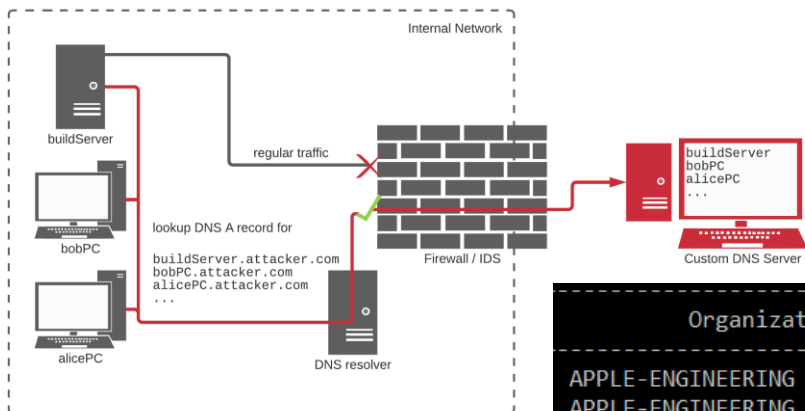
THE
DEVELOPER'S
CONFERENCE



Alex Birsan



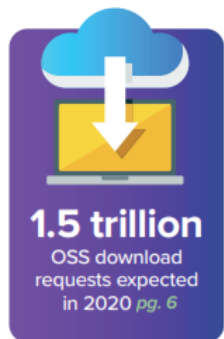
THE DEVELOPER'S CONFERENCE



373,000

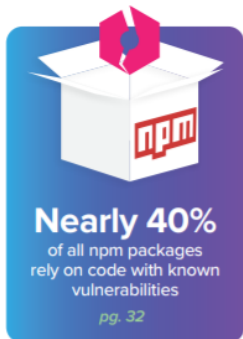
average enterprise downloads
of OSS components per year

pg. 33



1.5 trillion

OSS download
requests expected
in 2020 pg. 6



Nearly 40%

of all npm packages
rely on code with known
vulnerabilities

pg. 32

Organization	IP Address	Package Name	Hostname
APPLE-ENGINEERING - Apple Inc.	17.149.2	@ids/ids-pmrpc	.lan
APPLE-ENGINEERING - Apple Inc.	17.171.	@ids/ids-pmrpc	8faa3092cc97
APPLE-ENGINEERING - Apple Inc.	17.122.	@ids/ids-pmrpc	91c057281d0f
APPLE-ENGINEERING - Apple Inc.	17.122.	@ids/ids-pmrpc	1f3cc975c67b
APPLE-ENGINEERING - Apple Inc.	17.171.1	@ids/ids-pmrpc	fe01f79c7146
APPLE-ENGINEERING - Apple Inc.	17.122.	@ids/ids-pmrpc	7df2bb892313
APPLE-ENGINEERING - Apple Inc.	17.171.1	@ids/ids-pmrpc	c6269b74ec56
APPLE-ENGINEERING - Apple Inc.	17.171.1	@ids/ids-pmrpc	580f8f68bad3
APPLE-ENGINEERING - Apple Inc.	17.122.	@ids/ids-pmrpc	d7bea26b6122
APPLE-ENGINEERING - Apple Inc.	17.171.	@ids/ids-pmrpc	f507d7c91170
APPLE-ENGINEERING - Apple Inc.	17.122.	@ids/ids-pmrpc	e0b80fce2ded
APPLE-ENGINEERING - Apple Inc.	17.122.	@ids/ids-pmrpc	fab9b33c62b4
APPLE-ENGINEERING - Apple Inc.	17.122.	@ids/ids-pmrpc	dfec8557ad01
APPLE-ENGINEERING - Apple Inc.	17.171.	@ids/ids-pmrpc	23495738a747

Alex Birsan



THE
DEVELOPER'S
CONFERENCE



3 Ways to Mitigate Risk When Using Private Package Feeds

Secure Your Hybrid Software Supply Chain

Latest version located at: <https://aka.ms/pkg-sec-wg>

	How to handle multiple indexes	Our recommended configuration	Best practice			
Gradle	Gradle only uses explicitly listed repositories but will select any with the best available version.	Specify a single private Maven repository and enable upstreams on the private repository.				
Maven Central	Multiple repository URLs can be specified in user or project profiles. These are queried in order, though the order is not obvious from any one configuration file.	Specify a single mirror for all repositories, to ensure your private repository takes priority. Enable upstreams on the private repository.				
			npm	Registries are linked to a package name scope, making npm safe for properly scoped packages.	Either use scopes for all private packages or override the default registry with your private registry and enable upstreams.	Also include package-lock.json with your sources and use "npm ci" to install matching packages without performing any upgrades.
			NuGet Gallery	Multiple package sources specified by user or project. Latest version from any source will be installed.	Clear all packageSource settings in project configuration or nuget.config, add only your private gallery, and enable upstreams.	Prefer the "nuget restore -locked-mode" command and include a generated packages.lock.json with your project.
			Pip	One default package index and multiple extra index URLs. Latest version from any index will be installed.	Use pip's index-url setting to specify your private index and enable upstreams. Avoid extra-index-url.	Use "pip-compile" to generate locked file with hashes and enable hash-checking mode when installing.
			Yarn	Registries are linked to a package name scope, making Yarn safe for properly scoped packages.	Either use scopes for all private packages or override the default registry with your private registry and enable upstreams.	Also include yarn.lock with your sources and use "yarn install --immutable --immutable-cache --check-cache" to ensure matching packages are present.

<https://azure.microsoft.com/pt-br/resources/3-ways-to-mitigate-risk-using-private-package-feeds/>

Dependency Track



THE
DEVELOPER'S
CONFERENCE



Objetivo da plataforma



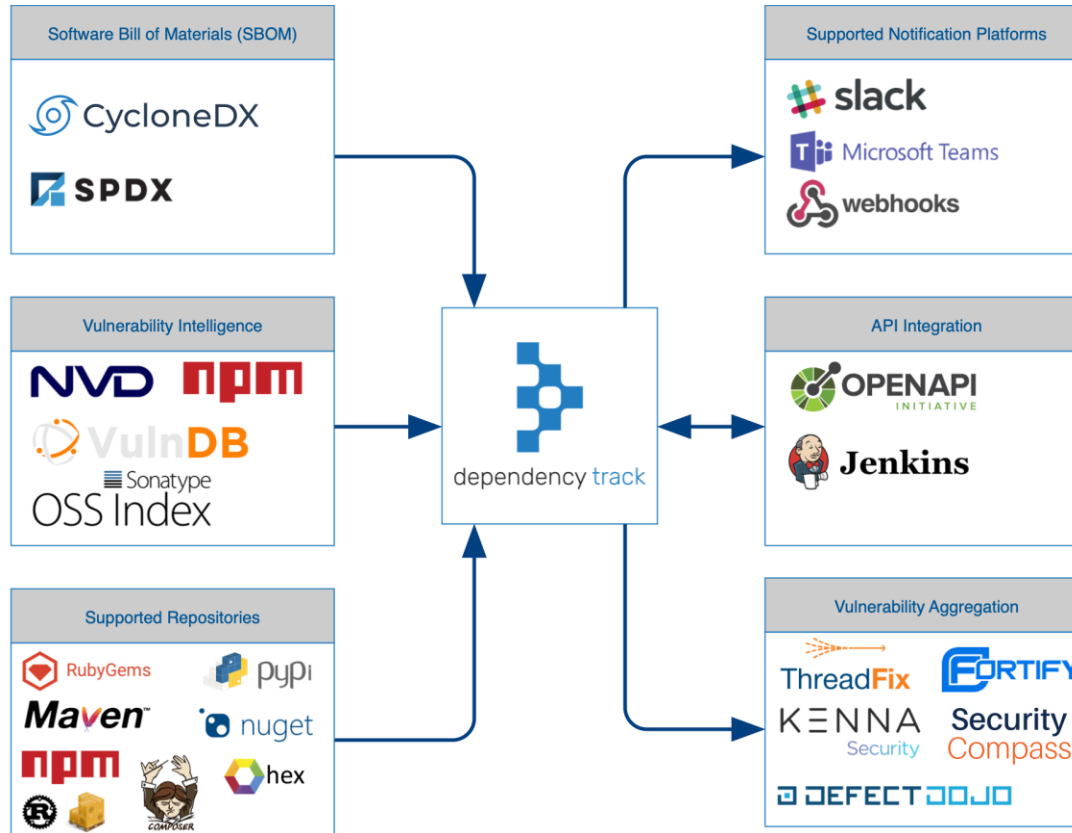
- Reduzir o risco da cadeia de componentes de terceiros.
- Permite a criação de políticas para validar:
 - Licenças
 - Segurança
 - Operacional
- Analise de impacto
- Notificação (webhooks)
- Fornece API para integrações
- Versão nova 4.2.1 (03/2021)



Ecosystema



THE
DEVELOPER'S
CONFERENCE



CycloneDX



THE
DEVELOPER'S
CONFERENCE

Tool Center

Show all Open source Proprietary Build integration Analysis Author GitHub action Transform Library

opensource build-integration

Auditjs

Sonatype

Audits an NPM package.json file to identify known vulnerabilities

Fork 34 Stars 134

opensource build-integration

Chelsea

Sonatype

Dependency vulnerability auditor for Ruby

Fork 3 Stars 7

proprietary analysis transform

CyberProtek

MedisAO

CyberProtek is an SBOM generation and translation tool for IoT that scans code metadata to create SBOMs, translates between SWID/SPDX/CycloneDx and manages vulnerabilities

opensource github-action

CycloneDX .NET Generate SBOM

CycloneDX

Creates CycloneDX SBOMs from .NET projects via GitHub action

Fork 0 Stars 1

opensource transform

CycloneDX CLI

CycloneDX

A command line tool incorporating many common utilities including converting between SBOM formats.

Fork 2 Stars 10

opensource library

CycloneDX Core for Java

CycloneDX

Library which facilitates the creation of SBOMs from Java objects, parsing of existing SBOMs into an object model, and validation of SBOMs

Fork 11 Stars 17

```
{
  "bomFormat": "CycloneDX",
  "specVersion": "1.2",
  "serialNumber": "urn:uuid:3e671687-395b-41f5-a30f-a58921a69b79",
  "version": 1,
  "components": [
    {
      "type": "application",
      "name": "Acme Application",
      "version": "9.1.1",
      "cpe": "cpe:/a:acme:application:9.1.1",
      "swid": {
        "tagId": "swidgen-242eb18a-503e-ca37-393b-cf156ef09691_9.1.1",
        "name": "Acme Application",
        "version": "9.1.1",
        "text": {
          "contentType": "text/xml",
          "encoding": "base64",
          "content": "PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0idXRmLTgiID8="
        }
      }
    },
    {
      "type": "library",
      "group": "org.apache.tomcat",
      "name": "tomcat-catalina",
      "version": "9.0.14",
      "purl": "pkg:maven/org.apache.tomcat/tomcat-catalina@9.0.14"
    }
  ]
}
```

<https://cyclonedx.org/tool-center/>

Script



THE
DEVELOPER'S
CONFERENCE

```
--${{if in(parameters.technology, 'angular', 'angularjs', 'node-app', 'node-package', 'reactjs', 'reactnative', 'vue')}}:
...-script: |
...  pwd
...  ls -la

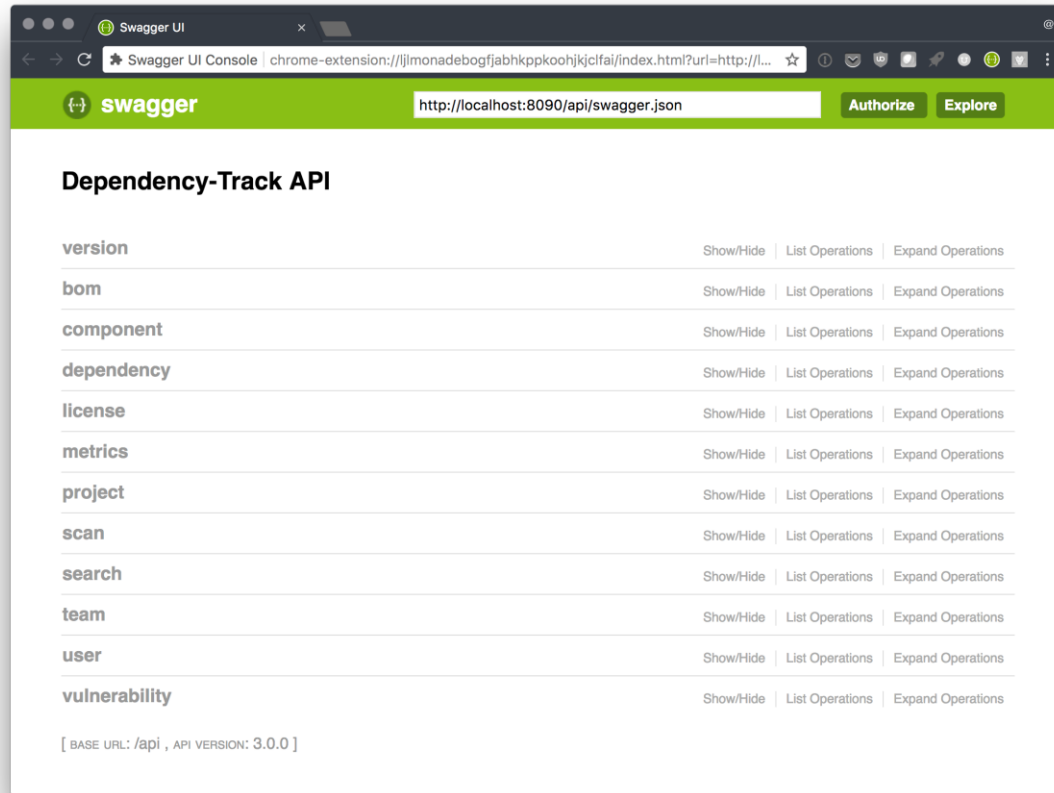
...  npx -p @cyclonedx/bom cyclonedx-bom -d
...-displayName: Run CycloneDX
...-workingDirectory: $(System.DefaultWorkingDirectory)

--${{if eq(parameters.technology, 'dotnetcore')}}:
...-task: PowerShell@2
...  name: processing
...  displayName: Processing
...  inputs:
...    targetType: 'inline'
...    script: |
...      $sln = Get-ChildItem -recurse | Where-Object -FilterScript {$_ .Name -match "Wiz.*.sln"} | Select-Object FullName, DirectoryName -f 1
...
...      cd $sln.DirectoryName
...      pwd
...
...      Write-Output "$($sln)"
...
...      dotnet tool restore
...
...      Write-Output 'Restored'
...
...      dotnet tool run dotnet-CycloneDX $sln.FullName -o ./
```

API First



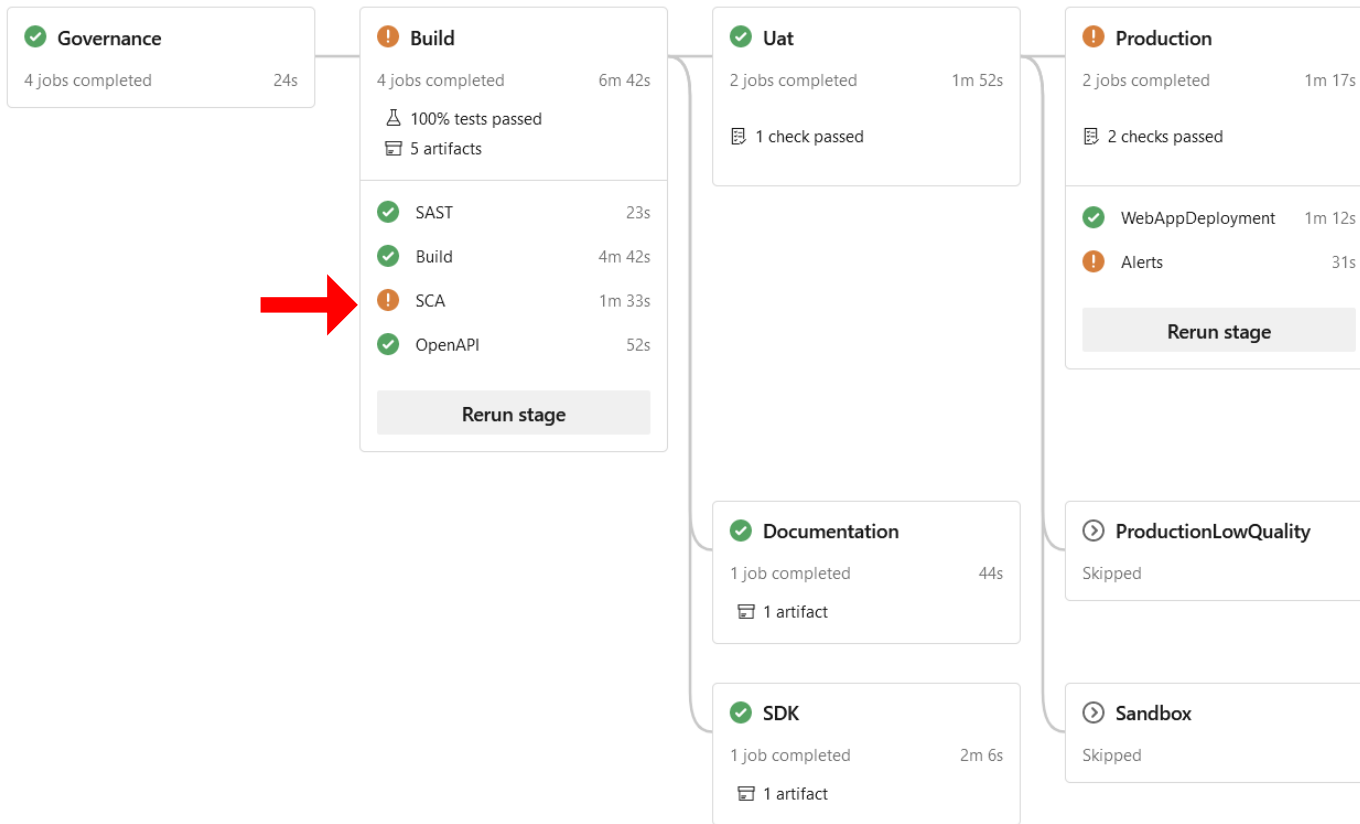
THE
DEVELOPER'S
CONFERENCE



Fácil integração



THE
DEVELOPER'S
CONFERENCE



Projetos



THE
DEVELOPER'S
CONFERENCE

[Home](#) / [Projects](#)

9
Portfolio Vulnerabilities



1
Projects at Risk



2
Vulnerable Components



41
Inherited Risk Score



[+ Create Project](#)



× Show inactive projects

Search




Project Name	Version	Last BOM Import	BOM Format	Risk Score	Active	Vulnerabilities
ap		25 Mar 2021 at 15:03:01	CycloneDX 1.2	5	<input checked="" type="checkbox"/>	<div><div>1</div></div>
ap		17 Mar 2021 at 12:04:58	CycloneDX 1.2	59	<input checked="" type="checkbox"/>	<div><div>10</div><div>3</div></div>
ap		23 Mar 2021 at 18:44:21	CycloneDX 1.2	41	<input checked="" type="checkbox"/>	<div><div>7</div><div>2</div></div>
ap		8 Mar 2021 at 15:28:02	CycloneDX 1.2	5	<input checked="" type="checkbox"/>	<div><div>1</div></div>
ap		4 Mar 2021 at 22:48:59	CycloneDX 1.2	5	<input checked="" type="checkbox"/>	<div><div>1</div></div>
ba	i	4 Mar 2021 at 18:35:02	CycloneDX 1.2	77	<input checked="" type="checkbox"/>	<div><div>12</div><div>4</div><div>1</div></div>
ba	b	24 Mar 2021 at 17:23:34	CycloneDX 1.2	145	<input checked="" type="checkbox"/>	<div><div>17</div><div>15</div><div>5</div><div>2</div></div>

Projetos



Home / Projects / habitacional-web

 .web

1

2


0


0


0

[View Details](#)

Overview

 **Components** 1429


 Audit Vulnerabilities 3

 Policy Violations 3

[+ Add Component](#)

[- Remove Component](#)

[Upload BOM](#)

 ▼

■	Component	Version		Group	Internal	License	Risk Score	Vulnerabilities
■	abab	2.0.5	▲			BSD-3-Clause	0	<div>0</div>
■	abbrev	1.1.1	▲			ISC	0	<div>0</div>
■	accepts	1.3.7	▲			MIT	0	<div>0</div>
■	acorn	6.4.2	▲			MIT	0	<div>0</div>
■	address	4.1.0	▲	@hapi		BSD-3-Clause	0	<div>0</div>
■	adjust-sourcemap-loader	3.0.0	▲			MIT	0	<div>0</div>
■	adm-zip	0.4.16	▲			MIT	0	<div>0</div>

Risk: Outdated component.
Current version is: 4.0.0

Projetos



Home / Projects / habitacional-web



-web



View Details

Overview

Components 1429

Audit Vulnerabilities 3

Policy Violations 3

☐ Show suppressed findings

Search




	Component	Version	Group	Vulnerability	Severity	Analyzer	Attributed On	Analysis	Suppressed
>	engine.io	3.5.0		NVD CVE-2020-36048	High	OSS Index	9 Mar 2021		
>	socket.io-parser	3.3.2		NVD CVE-2020-36049	High	OSS Index	9 Mar 2021		
>	core	9.0.0	@angular	OSSINDEX 1d5ccd1a-058b-4d88-b765-caa366edc62b	Critical	OSS Index	9 Mar 2021		

Showing 1 to 3 of 3 rows

Projetos: auditoria



Home / Projects / habitacional-web

 -web

1

2

0

0

0

[View Details](#)

Overview

Components **1429**

Audit Vulnerabilities **3**

Policy Violations **3**

☐ x Show suppressed violations

	State	Risk Type	Policy Name	Component	Occurred On	Analysis	Suppressed
>	FAIL	Security	Bugs nos apps	core 9.0.0	19 Mar 2021		
>	FAIL	Security	Bugs nos apps	socket.io-parser 3.3.2	19 Mar 2021		
>	FAIL	Security	Bugs nos apps	engine.io 3.5.0	19 Mar 2021		

Showing 1 to 3 of 3 rows

Projetos: auditoria



	State	Risk Type	Policy Name	Component	Occurred On	Analysis	Suppressed
▼	FAIL	Security	Bugs nos apps	core 9.0.0	19 Mar 2021	NOT_SET	

Condition

subject == SEVERITY && value IS CRITICAL

Audit Trail

admin - 25 Mar 2021 at 15:11:50
NOT_SET → APPROVED

admin - 25 Mar 2021 at 15:11:53
APPROVED → NOT_SET

admin - 25 Mar 2021 at 15:12:13
O dev vai alterar a lib

Comment

Add Comment

Analysis

Not Set

Suppress

Políticas



[Home](#) / Policy Management

 Policies 1

 License Groups 4

[+ Create Policy](#)



FAIL Bugs nos apps

Name *

Bugs nos apps



Operator *

Any



Violation State *

Fail



Conditions

Severity



is



High



Severity



is



Critical



[▼ Limit To](#)

[Delete Policy](#)


Políticas



THE
DEVELOPER'S
CONFERENCE

[Home](#) / Policy Management

 Policies 2

 License Groups 4

[+ Create Policy](#)



FAIL Bugs nos apps

FAIL Licença comercial

Name *

Licença comercial

Operator *

Any

Violation State *

Fail

Conditions

License group

is not

Permissive

Severity

Coordinates

License

License group

Package URL (PURL)

Common Platform Enumeration (CPE)

SWID Tag ID

 Limit To

Delete Policy


Showing

Politicas



[Home](#) / Policy Management

 Policies 2

 License Groups 4

[+ Create License Group](#)

Search



Copyleft

Non-Commercial

Permissive

Name *

Permissive



Licenses

Apache License 1.0



Apache License 1.1



Apache License 2.0



Boost Software License 1.0



BSD-2-Clause Plus Patent License



Vulnerabilidades



Name	Published	CWE	Projects	Severity
NPM 1598	25 Jan 2021	CWE-506 Embedded Malicious Code	0	Critical
NPM 1597	25 Jan 2021	CWE-506 Embedded Malicious Code	0	Critical
NPM 1596	25 Jan 2021	CWE-506 Embedded Malicious Code	0	Critical
NPM 1595	6 Jan 2021	CWE-20 Improper Input Validation	0	Medium
NPM 1594	4 Jan 2021	CWE-918 Server-Side Request Forgery (SSRF)	1	High
NPM 1593	30 Dec 2020	CWE-312 Cleartext Storage of Sensitive Information	0	Low
NPM 1592	30 Dec 2020	CWE-400 Uncontrolled Resource Consumption	0	Medium
NPM 1591	18 Dec 2020	CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	0	Medium
NPM 1590	16 Dec 2020	CWE-78 Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	0	Medium
NPM 1589	9 Dec 2020	CWE-471 Modification of Assumed-Immutable Data (MAID)	16	Low
NPM 1588	8 Dec 2020	CWE-400 Uncontrolled Resource Consumption	0	Low
NPM 1587	8 Dec 2020	CWE-400 Uncontrolled Resource Consumption	0	Low
NPM 1586	4 Dec 2020	CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	0	High
NPM 1585	30 Nov 2020	CWE-506 Embedded Malicious Code	0	Critical

Vulnerabilidades



[Home](#) / [Vulnerabilities](#) / 1594 (NPM)



1594 (NPM)

NPM Advisories


Server-Side Request Forgery




High Severity

[View Details](#)



 Overview

 Affected Projects 1

Overview

The `axios` NPM package before 0.21.1 contains a Server-Side Request Forgery (SSRF) vulnerability where an attacker is able to bypass a proxy by providing a URL that responds with a redirect to a restricted host or IP address.

Weakness

CWE-918: Server-Side Request Forgery (SSRF)

Recommendation

Upgrade to 0.21.1 or later.

Vulnerabilidades



[Home](#) / [Vulnerabilities](#) / 1594 (NPM)



1594 (NPM)

NPM Advisories
Server-Side Request Forgery



High Severity

[View Details](#)



[Overview](#)

[Affected Projects](#)

1



Name



Version



[vendasWeb](#)

-

Showing 1 to 1 of 1 rows

Vulnerabilidades



Home > CWE List > CWE- Individual Dictionary Definition (4.4)

ID Lookup: Go

[Home](#) | [About](#) | [CWE List](#) | [Scoring](#) | [Community](#) | [News](#) | [Search](#)

CWE-918: Server-Side Request Forgery (SSRF)

Weakness ID: 918

Abstraction: Base

Structure: Simple

Status: Incomplete

Presentation Filter:

▼ Description

The web server receives a URL or similar request from an upstream component and retrieves the contents of this URL, but it does not sufficiently ensure that the request is being sent to the expected destination.

▼ Extended Description

By providing URLs to unexpected hosts or ports, attackers can make it appear that the server is sending the request, possibly bypassing access controls such as firewalls that prevent the attackers from accessing the URLs directly. The server can be used as a proxy to conduct port scanning of hosts in internal networks, use other URLs such as that can access documents on the system (using file://), or use other protocols such as gopher:// or tftp://, which may provide greater control over the contents of requests.

▼ Alternate Terms

XSPA: Cross Site Port Attack

▼ Relationships

The table(s) below shows the weaknesses and high level categories that are related to this weakness. These relationships are defined as ChildOf, ParentOf, MemberOf and give insight to similar items that may exist at higher and lower levels of abstraction. In addition, relationships such as PeerOf and CanAlsoBe are defined to show similar weaknesses that the user wants to explore.

Bases externas



THE
DEVELOPER'S
CONFERENCE

[Home](#) / Administration

≡ **Configuration**

≡ **Analyzers**

Internal

NPM Audit

Sonatype OSS Index

VulnDB

≡ **Repositories**

≡ **Notifications**

≡ **Integrations**

≡ **Access Management**

Internal



Enable internal analyzer

The internal analyzer evaluates components against an internal vulnerability database derived from the National Vulnerability Database and VulnDB (if enabled). This analyzer makes use of the Common Platform Enumeration (CPE) defined in components. Components with a valid CPE will be evaluated with this analyzer.

Update

Repositorios



Configuration

Analyzers

Repositories

Cargo

Composer

Gem

Hex

Maven

NPM

NuGet

Python

NuGet

+ Create Repository

Search

↺

Identifier	URL	Internal	Enabled
nuget-gallery	https://api.nuget.org/		<input checked="" type="checkbox"/>

Showing 1 to 1 of 1 rows

Notificações



THE
DEVELOPER'S
CONFERENCE

[Home](#) / Administration

≡ Configuration

≡ Analyzers

≡ Repositories

≡ Notifications

Alerts

Templates

≡ Integrations

≡ Access Management

Templates

Name

Console

Email

Microsoft Teams

Outbound Webhook

Slack

Showing 1 to 5 of 5 rows

Search



Default

Dependency Track terça-feira 15:59

New Vulnerability Identified



Dependency-Track

03/23/2021 18:59:02

elliptic before version 6.5.4 is vulnerable to Cryptographic Issues via the secp256k1 implementation in elliptic/ec/key.js. There is no check to confirm that the public key point passed into the derive function actually exists on the secp256k1 curve. This results in the potential for the private key used in this implementation to be revealed after a number of ECDH operations are performed.

VulnID 1648
Severity MEDIUM
Source NPM
Component pkg:npm/elliptic@6.5.2

← Responder

Integrações nativas



≡ Configuration

≡ Analyzers

≡ Repositories

≡ Notifications

≡ Integrations

Fortify SSC

DefectDojo

Kenna Security

≡ Access Management

Fortify SSC

☐ × Enable Fortify SSC integration

Synchronization cadence (in minutes)

60

Restarting Dependency-Track is required for cadence changes to take effect

URL

URL

Username

Username

Password

.....

Update

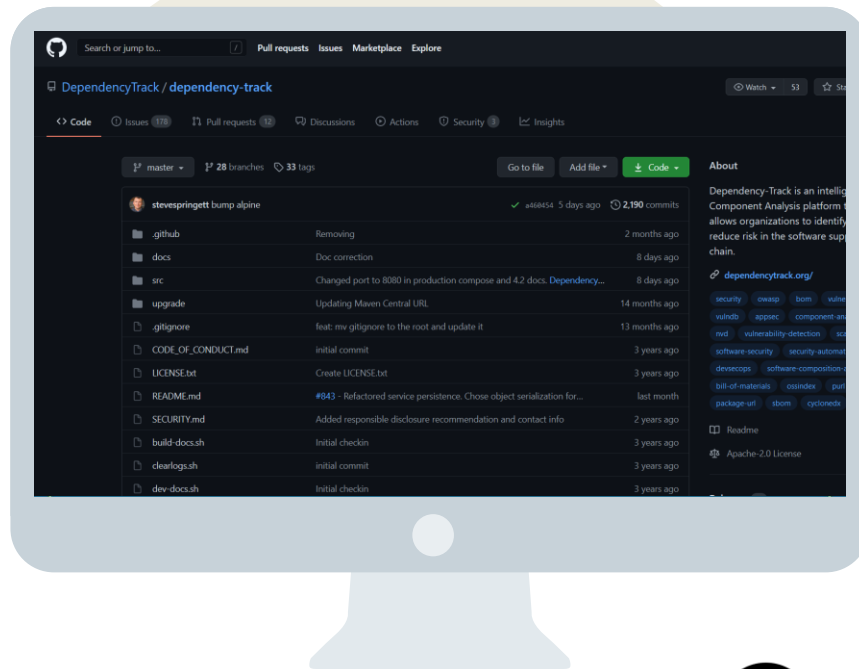
Mais informação



THE
DEVELOPER'S
CONFERENCE

<https://github.com/DependencyTrack/dependency-track>

<https://hub.docker.com/r/dependencytrack/bundled>





THE DEVELOPER'S CONFERENCE