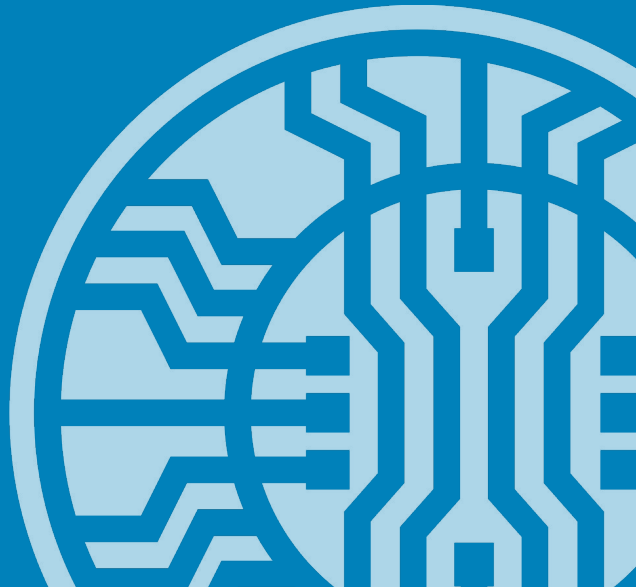
Ostorlab

Mobile Security & 3rd Party Dependency Security

Alaeddine Mesbahi
alaeddine.mesbahi@ostorlab.dev
@3asm_

26-06-2020

The story of a bug ...



cordova-plugin-advanced-http

2.5.1 • Public • Published 21 days ago

Readme | Explore BETA | 0 Dependencies | 4 Dependents | 45 Versions

Cordova Advanced HTTP

Cordova / Phonegap plugin for communicating with HTTP servers. Supports iOS, Android and Browser.

This is a fork of Wymsee's Cordova-HTTP plugin.

Advantages over Javascript requests

- SSL / TLS Pinning
- CORS restrictions do not apply
- X.509 client certificate based authentication
- Handling of HTTP code 401 - read more at Issue CB-2415

Updates

Please check CHANGELOG.md for details about updating to a new version.

Installation

The plugin conforms to the Cordova plugin specification, it can be installed using the Cordova / Phonegap command line interface.

```
phonegap plugin add cordova-plugin-advanced-http

cordova plugin add cordova-plugin-advanced-http
```

Usage

Plain Cordova

This plugin registers a global object located at `cordova.plugin.http`.

With Ionic-native wrapper

Check the Ionic docs for how to use this plugin with Ionic-native.

Synchronous Functions

Install

```
npm i cordova-plugin-advanced-http
```

Weekly Downloads

12,234

Version	License
2.5.1	MIT

Unpacked Size	Total Files
830 kB	70

Issues	Pull Requests
29	3

Homepage

github.com/silkimen/cordova-plugin-ad...

Repository

github.com/silkimen/cordova-plugin-ad...

Last publish

21 days ago

Collaborators

Try on RunKit

Report a vulnerability

Security advisories

Advisory	Date of advisory	Status
Improper Verification of Cryptographic Signature jsrsasign severity moderate	Jun 23rd, 2020	status patched
Improper Authorization @sap-cloud-sdk/core severity high	Jun 17th, 2020	status patched
Remote Code Execution next severity high	Jun 9th, 2020	status patched
Information Exposure apollo-server-lambda severity moderate	Jun 5th, 2020	status patched
Information Exposure apollo-server-micro severity moderate	Jun 5th, 2020	status patched
Information Exposure apollo-server-koa severity moderate	Jun 5th, 2020	status patched
Information Exposure apollo-server-hapi severity moderate	Jun 5th, 2020	status patched

Overview

Security policy

Security advisories 0

Security overview

View security details for this repository

See security announcements from this repository's maintainers

Security policy

Suggest how users should report security vulnerabilities for this repository

Suggest a security policy

Security advisories

View security advisories for this repository

View security advisories

Tag: v2.0.6 **cordova-plugin-advanced-http** / src / android / com / github / kevinsawicki / **http** /

Go to file

silkimen committed `a0f3762` on 1 Mar 2019 ...

History

..

HttpRequest.java	Fix **#187**: setSSLCertMode with "default" throws an error on Android	16 months ago
OkConnectionFactory.java	refactored to use Singleton instance of ConnectionFactory	2 years ago
TLSSocketFactory.java	fixes **#79**	2 years ago

CVE-2019-1010206 Detail

Current Description

OSS Http Request (Apache Cordova Plugin) 6 is affected by: Missing SSL certificate validation. The impact is: certificate spoofing. The component is: use this library when https communication. The attack vector is: certificate spoofing.

Source: MITRE

+View Analysis Description

Severity

CVSS Version 3.x | CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NIST: NVD **Base Score:** 5.9 MEDIUM **Vector:** CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

Hyperlink	Resource
https://github.com/kevinsawicki/http-request/blob/master/lib/src/main/java/com/github/kevinsawicki/http/HttpRequest.java	Third Party Advisory

Weakness Enumeration

CWE-ID	CWE Name	Source
CWE-295	Improper Certificate Validation	NIST

Known Affected Software Configurations Switch to CPE 2.2

Configuration 1 (hide)

cpe:2.3:a:http_request_project:http_request:6.0:*:*:*:*:cordova:*:*

Show Matching CPE(s)

Mobile Application Security Scanner

Upload, Scan, Fix!

Scan

Android & iOS

Advanced Analysis

Detailed Report

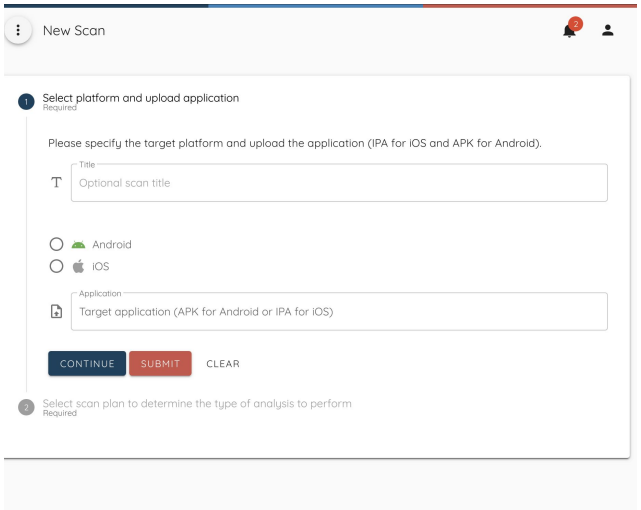
Last public scans

Package name
com.expressvpn.vpn
Version
8.0.1

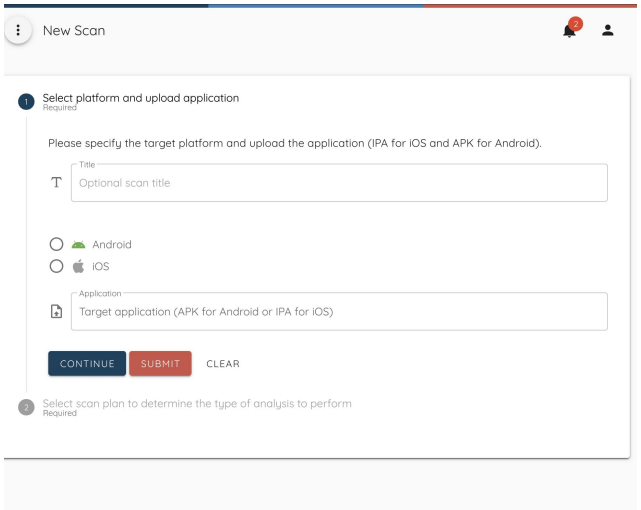
HIGH

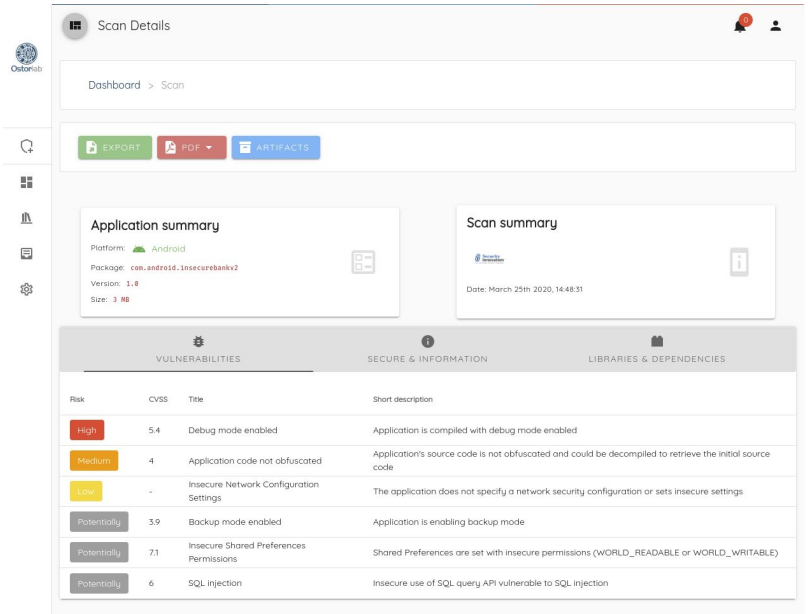
How does it work?

How does it work?

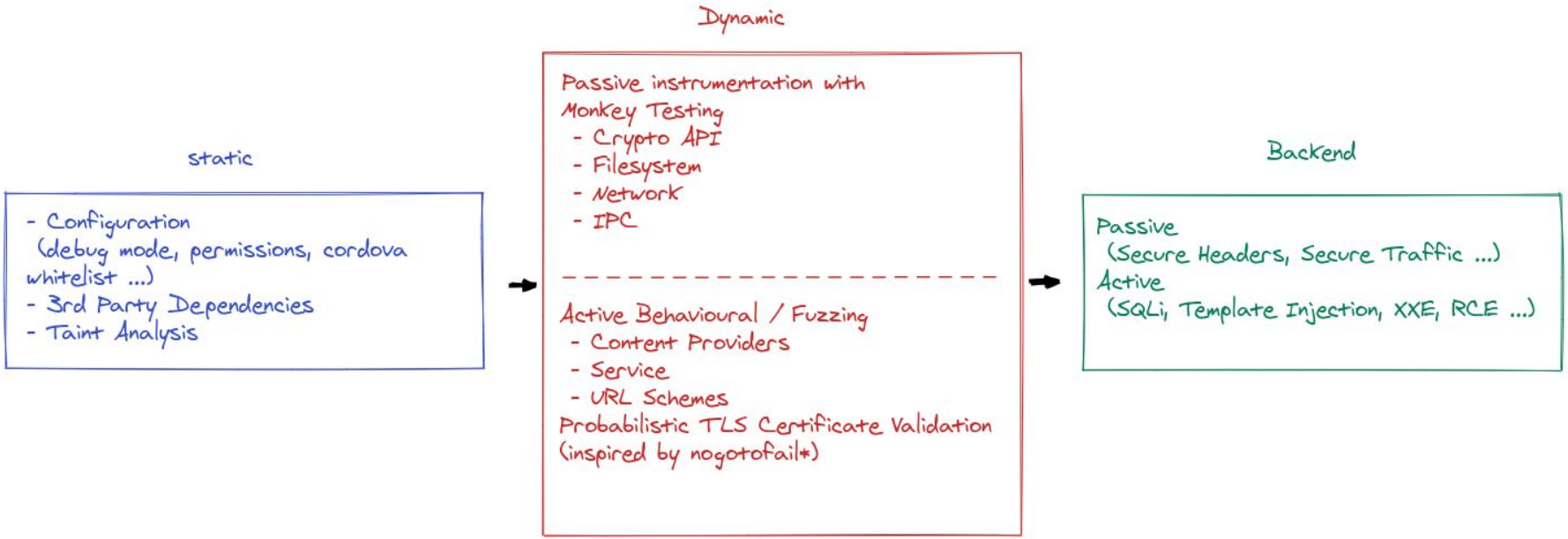


How does it work?

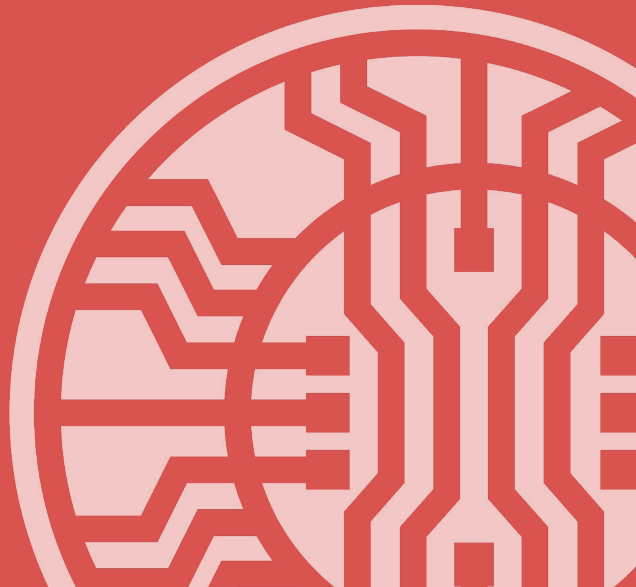




Stages of Analysis



How are 3rd Party Dependencies used?

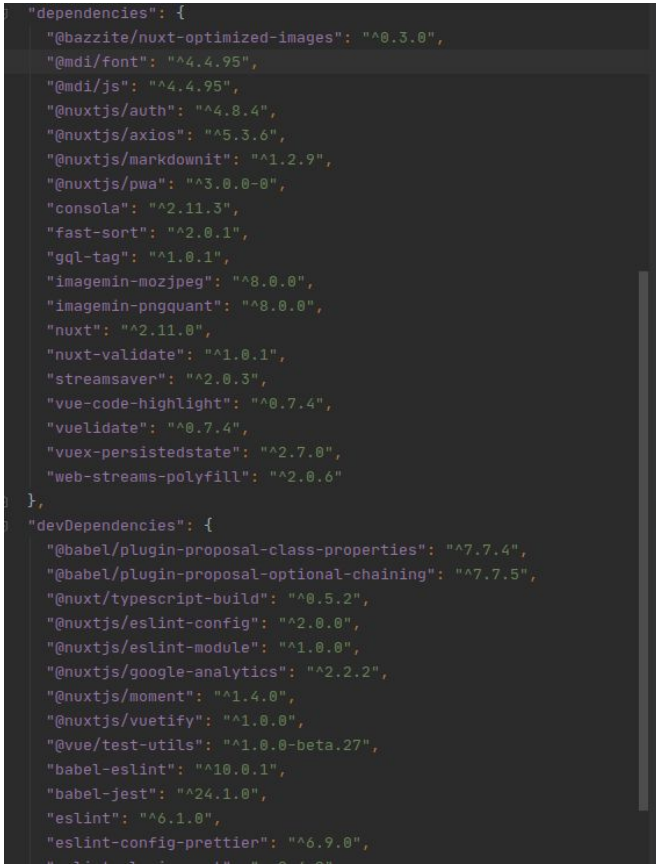


3rd Party Dependencies Security

3rd Party Dependencies Security

Copying code ...

package.json

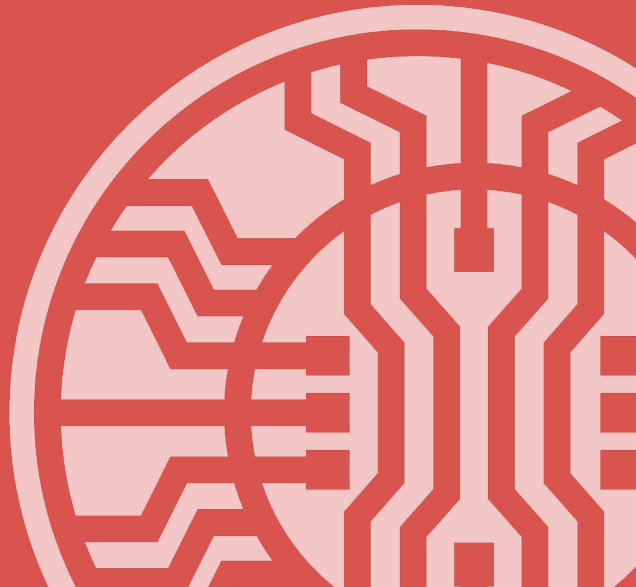


```
"dependencies": {
  "@bazzite/nuxt-optimized-images": "^0.3.0",
  "@mdi/font": "^4.4.95",
  "@mdi/js": "^4.4.95",
  "@nuxtjs/auth": "^4.8.4",
  "@nuxtjs/axios": "^5.3.6",
  "@nuxtjs/markdownit": "^1.2.9",
  "@nuxtjs/pwa": "^3.0.0-0",
  "consola": "^2.11.3",
  "fast-sort": "^2.0.1",
  "gql-tag": "^1.0.1",
  "imagemin-mozjpeg": "^8.0.0",
  "imagemin-pngquant": "^8.0.0",
  "nuxt": "^2.11.0",
  "nuxt-validate": "^1.0.1",
  "streamsaver": "^2.0.3",
  "vue-code-highlight": "^0.7.4",
  "vuelidate": "^0.7.4",
  "vuex-persistedstate": "^2.7.0",
  "web-streams-polyfill": "^2.0.6"
},
"devDependencies": {
  "@babel/plugin-proposal-class-properties": "^7.7.4",
  "@babel/plugin-proposal-optional-chaining": "^7.7.5",
  "@nuxt/typescript-build": "^0.5.2",
  "@nuxtjs/eslint-config": "^2.0.0",
  "@nuxtjs/eslint-module": "^1.0.0",
  "@nuxtjs/google-analytics": "^2.2.2",
  "@nuxtjs/moment": "^1.4.0",
  "@nuxtjs/vuetify": "^1.0.0",
  "@vue/test-utils": "^1.0.0-beta.27",
  "babel-eslint": "^10.0.1",
  "babel-jest": "^24.1.0",
  "eslint": "^6.1.0",
  "eslint-config-prettier": "^6.9.0",
```

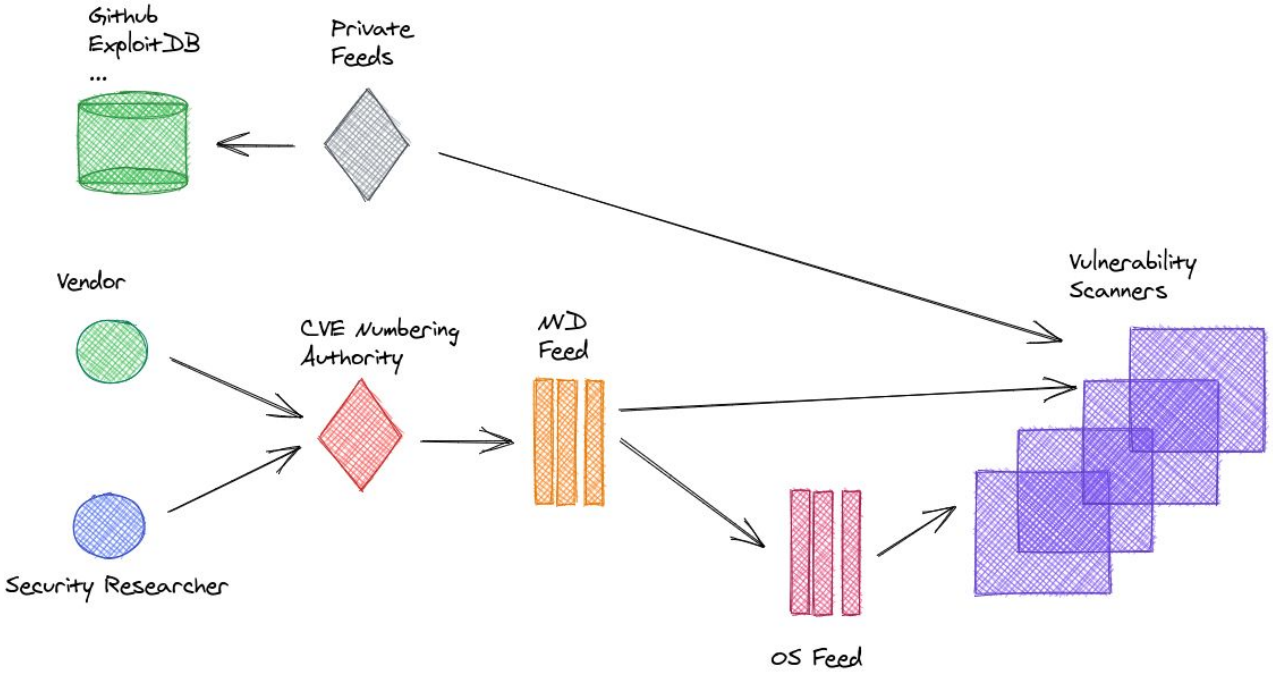
package-lock.json


```
61    "resolved": "https://registry.npmjs.org/@babel/generator/-/generator-7.7.7.tgz",
62    "integrity": "sha512-/AOIBpHh/JU1l0ZFS4kiRCBnLi6OTHzh0RPk3h9isBxkkqELtQNFi1Vr/tiG9p1yfoUdKVwISuXWQR+hwwM4VQ==",
63    "requires": {
64      "@babel/types": "^7.7.4",
65      "jsesc": "^2.5.1",
66      "lodash": "^4.17.13",
67      "source-map": "^0.5.0"
68    }
69  },
70  "@babel/helper-annotate-as-pure": {
71    "version": "7.7.4",
72    "resolved": "https://registry.npmjs.org/@babel/helper-annotate-as-pure/-/helper-annotate-as-pure-7.7.4.tgz",
73    "integrity": "sha512-2BQmQgECKzYKFPpiycoF9tlb5HA4lrVyAmLLVK177EcQAqjVLciUb2/R+n1boQ9y5ENV3uz2ZqiNw7QMBBw1Og==",
74    "requires": {
75      "@babel/types": "^7.7.4"
76    }
77  },
78  "@babel/helper-builder-binary-assignment-operator-visitor": {
79    "version": "7.7.4",
80    "resolved": "https://registry.npmjs.org/@babel/helper-builder-binary-assignment-operator-visitor/-/helper-builder-
81    "integrity": "sha512-Biq/d/WtvfftWZ9Uf39hbPBYDUo986m5Bb4zhkeYDGUllF43D+nUe5M6Vuo6/8JDK/0YX/uBdeoQpyaNhNugZQ==",
82    "requires": {
83      "@babel/helper-explode-assignable-expression": "^7.7.4",
84      "@babel/types": "^7.7.4"
85    }
86  },
87  "@babel/helper-call-delegate": {
88    "version": "7.7.4",
89    "resolved": "https://registry.npmjs.org/@babel/helper-call-delegate/-/helper-call-delegate-7.7.4.tgz",
90    "integrity": "sha512-8JH9/B7J7tCYJ2PpWVpw9JhPuEVHztagNVuQAFBVFYluRMlpG7F1CgKEgGeL6KFqcsIa92ZYVj6DSc0XwmN1ZA==",
91    "requires": {
92      "@babel/helper-hoist-variables": "^7.7.4",
93      "@babel/traverse": "^7.7.4",
94      "@babel/types": "^7.7.4"
95    }
```

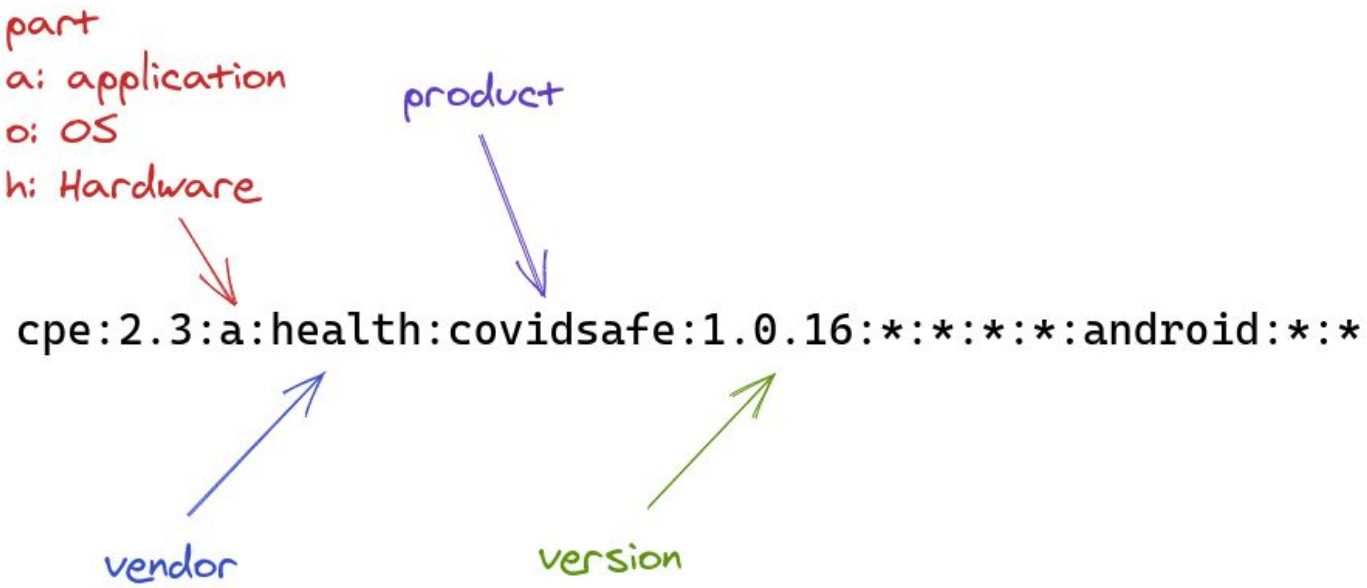
3rd Party Security Ecosystem



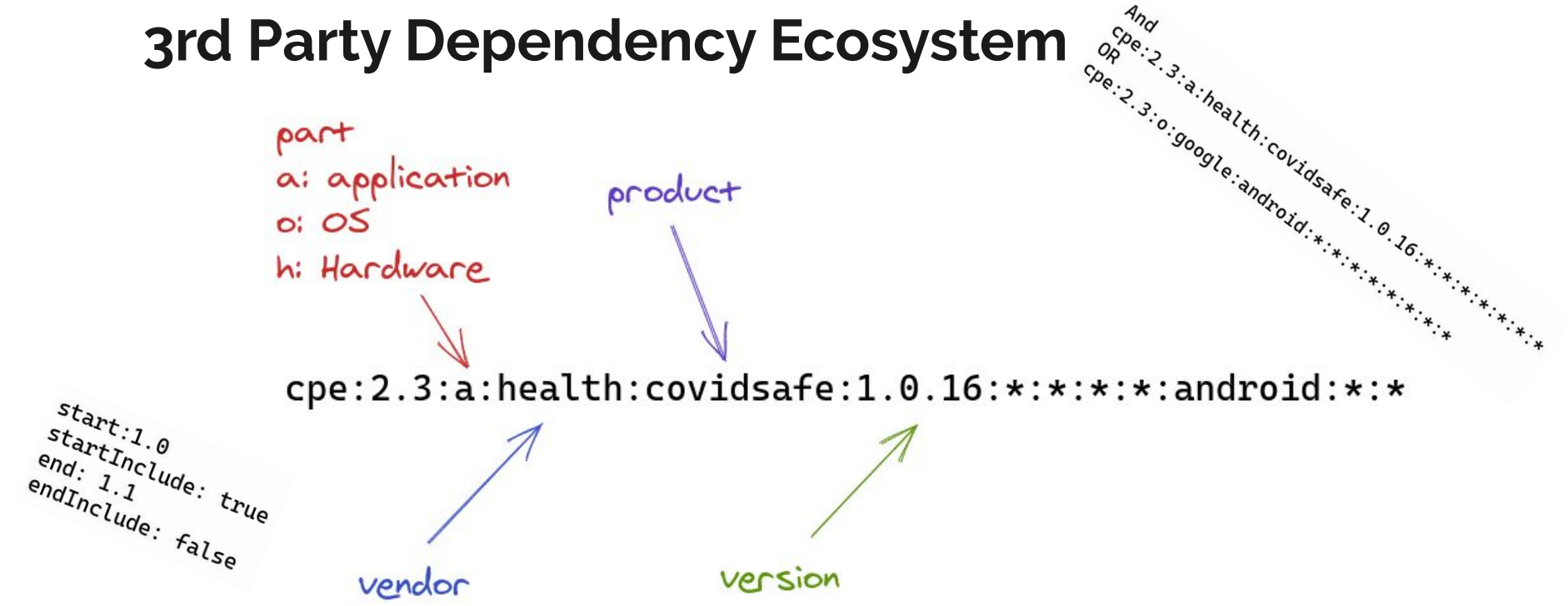
3rd Party Dependency Ecosystem



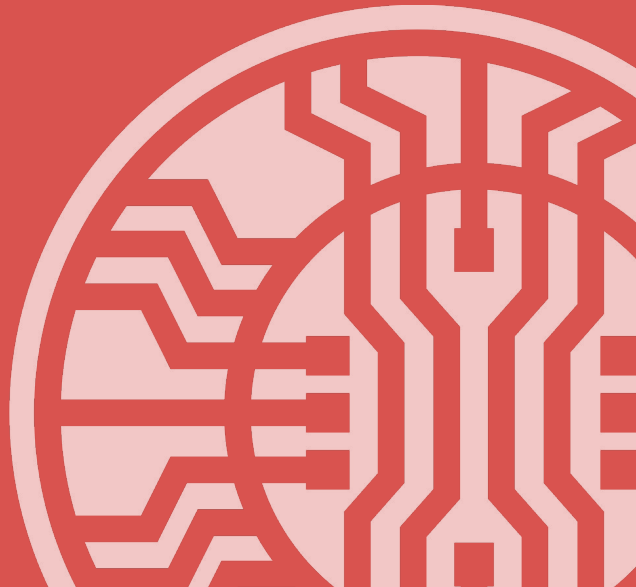
3rd Party Dependency Ecosystem



3rd Party Dependency Ecosystem



The Bad, The Ugly ...



CVE-2020-2530 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Current Description

Vulnerability in the Oracle HTTP Server product of Oracle Fusion Middleware (component: Web Listener). Supported versions that are affected are 11.1.1.9.0, 12.1.3.0.0 and 12.2.1.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle HTTP Server. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle HTTP Server, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle HTTP Server accessible data as well as unauthorized read access to a subset of Oracle HTTP Server accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).

Source: MITRE

View Analysis Description

Severity

CVSS Version 3.x | CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NIST: NVD	**Base Score:** 6.1 MEDIUM	**Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
CNA: Oracle	**Base Score:** 6.1 MEDIUM	**Vector:** CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

Hyperlink	Resource
https://www.oracle.com/security-alerts/cpujan2020.html	Patch, Vendor Advisory

Weakness Enumeration

CWE-ID	CWE Name	Source
NVD-CWE-noinfo	Insufficient Information	NIST

Known Affected Software Configurations Switch to CPE 2.2

Configuration 1 (hide)

cpe:2.3:a:apache:http_server:11.1.1.9.0:*:*:*:*:*:*:*

Hide Matching CPE(s)

- *cpe:2.3:a:apache:http_server:11.1.1.9.0:*:*:*:*:*:*:**

cpe:2.3:a:apache:http_server:12.1.3.0.0:*:*:*:*:*:*:*

Hide Matching CPE(s)

- *cpe:2.3:a:apache:http_server:12.1.3.0.0:*:*:*:*:*:*:**

cpe:2.3:a:apache:http_server:12.2.1.3.0:*:*:*:*:*:*:*

Hide Matching CPE(s)

- *cpe:2.3:a:apache:http_server:12.2.1.3.0:*:*:*:*:*:*:**

CVE-2019-12273 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Current Description

** DISPUTED ** OutSystems Platform 10 through 11 allows ImageResourceDetail.aspx CSRF for content modifications and file uploads. NOTE: The product is self-hosted by the customer, even though it has a *.outsystemsenterprise.com domain name.) NOTE: The vendor claims that the independent researcher created the report without any type of validation and that no such vulnerability exists.

Source: MITRE

View Analysis Description

Severity

CVSS Version 3.x | CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NIST: NVD **Base Score:** 6.5 MEDIUM **Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

Hyperlink	Resource
https://cxsecurity.com/issue/WLB-2019050242	Exploit, Third Party Advisory

Weakness Enumeration

CWE-ID	CWE Name	Source
CWE-352	Cross-Site Request Forgery (CSRF)	NIST

Known Affected Software Configurations Switch to CPE 2.2

Configuration 1 (hide)

cpe:2.3:a:outsystems:outsystems:*:*:*:*:*:*:*:*	From (including)	Up to (including)
Show Matching CPE(s)	10	11

List of Security Bulletins with Affected Version Changes

Security Bulletin	Previously announced Affected Releases	Updated Affected GA Releases	Minimum Fix GA Releases	CVE Identifiers
S2-002	2.0.0 - 2.0.11	2.0.0 - 2.1.8.1	2.2.1	
S2-003	2.0.0 - 2.0.11.2	2.0.0 - 2.1.8.1	2.2.1	CVE-2008-6504
S2-004	2.0.0 - 2.0.11.2	2.0.0 - 2.0.11.2 2.1.0 - 2.1.2	2.0.12 2.1.6	CVE-2008-6505
S2-008	2.1.0 - 2.3.1	2.0.0 - 2.2.3 2.0.0 - 2.3.17	2.2.3.1 2.3.18	CVE-2012-0391 CVE-2012-0394
S2-012	Struts Showcase App 2.0.0 - 2.3.13	2.0.0 - 2.3.14.2	2.3.14.3	CVE-2013-1965
S2-013	2.0.0 - 2.3.13	2.0.0 - 2.3.14.1	2.3.14.2	CVE-2013-1966
S2-020	2.0.0 - 2.3.16	2.0.0 - 2.3.16.1	2.3.16.2	CVE-2014-0094
S2-021	2.0.0 - 2.3.16.1	2.0.0 - 2.3.16.3	2.3.20	CVE-2014-0112 CVE-2014-0113
S2-022	2.0.0 - 2.3.16.1	2.0.0 - 2.3.16.3	2.3.20	CVE-2014-0116
S2-041	2.3.20 - 2.3.28.1 2.5	2.3.20 - 2.3.28.1 2.5 - 2.5.12	2.3.29 2.5.13	CVE-2016-4465
S2-042	2.3.20 - 2.3.30	2.3.1-2.3.30 2.5 - 2.5.2	2.3.31 2.5.5	CVE-2016-6795
S2-044	2.5 - 2.5.5	2.5 - 2.5.12	2.5.13	CVE-2016-8738
S2-048	Struts Showcase App 2.3.x	2.1.x - 2.3.x	-	CVE-2017-9791
S2-051	2.3.7 - 2.3.33 2.5 - 2.5.12	2.1.6 - 2.3.33 2.5 - 2.5.12	2.3.34 2.5.13	CVE-2017-9793
S2-053	2.0.1-2.3.33 2.5-2.5.10	2.0.0-2.3.33 2.5-2.5.10.1	2.3.34 2.5.12	CVE-2017-12611

Weakness Enumeration

CWE-ID	CWE Name	Source
CWE-20	Improper Input Validation	NIST

Known Affected Software Configurations Switch to CPE 2.2

Configuration 1 (hide)

- **cpe:2.3:a:apache:struts:2.3.7:*:*:*:*:*:*:***
  Show Matching CPE(s)
- **cpe:2.3:a:apache:struts:2.3.8:*:*:*:*:*:*:***
  Show Matching CPE(s)
- **cpe:2.3:a:apache:struts:2.3.9:*:*:*:*:*:*:***
  Show Matching CPE(s)
- **cpe:2.3:a:apache:struts:2.3.10:*:*:*:*:*:*:***
  Show Matching CPE(s)
- **cpe:2.3:a:apache:struts:2.3.11:*:*:*:*:*:*:***
  Show Matching CPE(s)
- **cpe:2.3:a:apache:struts:2.3.12:*:*:*:*:*:*:***
  Show Matching CPE(s)
- **cpe:2.3:a:apache:struts:2.3.13:*:*:*:*:*:*:***
  Show Matching CPE(s)
- **cpe:2.3:a:apache:struts:2.3.14:*:*:*:*:*:*:***
  Show Matching CPE(s)
- **cpe:2.3:a:apache:struts:2.3.14.1:*:*:*:*:*:*:***
  Show Matching CPE(s)
- **cpe:2.3:a:apache:struts:2.3.14.2:*:*:*:*:*:*:***
  Show Matching CPE(s)
- **cpe:2.3:a:apache:struts:2.3.14.3:*:*:*:*:*:*:***
  Show Matching CPE(s)
- **cpe:2.3:a:apache:struts:2.3.15:*:*:*:*:*:*:***
  Show Matching CPE(s)
- **cpe:2.3:a:apache:struts:2.3.15.1:*:*:*:*:*:*:***
  Show Matching CPE(s)

CVE-2019-1010091 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Current Description

tinymce 4.7.11, 4.7.12 is affected by: CWE-79: Improper Neutralization of Input During Web Page Generation. The impact is: JavaScript code execution. The component is: Media element. The attack vector is: The victim must paste malicious content to media element's embed tab.

Source: MITRE

+View Analysis Description

Severity

CVSS Version 3.x | CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NIST: NVD **Base Score:** 6.1 MEDIUM **Vector:** CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

Hyperlink	Resource
https://github.com/tinymce/tinymce/issues/4394	Exploit, Third Party Advisory

Weakness Enumeration

CWE-ID	CWE Name	Source
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	NIST DWF

Known Affected Software Configurations Switch to CPE 2.2

Configuration 1 (hide)

- **cpe:2.3:a:tiny.cloud:tinymce:4.7.11:*:*:*:*:*:*:***
  Show Matching CPE(s)
- **cpe:2.3:a:tiny.cloud:tinymce:4.7.12:*:*:*:*:*:*:***
  Show Matching CPE(s)

TinyMCE 5.2.2

Release notes for TinyMCE 5.2.2

Overview

These release notes provide an overview of the changes for TinyMCE 5.2.2, including:

- General bug fixes
- Security fixes
- Accompanying Premium Plugin changes
- Upgrading to the latest version of TinyMCE 5

> *This is the Tiny Cloud and TinyMCE Enterprise release notes. For information on the latest community version of TinyMCE, see: TinyMCE Changelog.*

General bug fixes

TinyMCE 5.2.2 provides fixes for the following bugs:

- Fixed an issue where anchors could not be inserted on empty lines.
- Fixed text decorations (underline, strikethrough) not consistently inheriting the text color.
- Fixed `format` menu alignment buttons inconsistently applying to images.
- Fixed the floating toolbar drawer height collapsing when the editor is rendered in modal dialogs or floating containers.

Security fixes

TinyMCE 5.2.2 provides fixes for the following security issues:

- Fixed `media` embed content not processing safely in some cases.

XSS in TinyMCE

moderate severity **CVE-2019-1010091** published on 11 May • updated 8 days ago

Repository	Packages	Affected versions	Patched versions
tinymce/tinymce	tinymce (npm)	< 4.9.10 >= 5.0.0, < 5.2.2	4.9.10 5.2.2

Impact

A cross-site scripting (XSS) vulnerability was discovered in: the core parser and `media` plugin. The vulnerability allowed arbitrary JavaScript execution when inserting a specially crafted piece of content into the editor via the clipboard or APIs. This impacts all users who are using TinyMCE 4.9.9 or lower and TinyMCE 5.2.1 or lower.

Patches

This vulnerability has been patched in TinyMCE 4.9.10 and 5.2.2 by improved HTML parsing and sanitization logic.

Workarounds

The workarounds available are:

- disable the media plugin and manually sanitize CDATA content (see below)
  or
- upgrade to either TinyMCE 4.9.10 or TinyMCE 5.2.2

Example: Manually strip CDATA elements

```
setup: function(editor) {
  editor.on('PreInit', function() {
    editor.parser.addNodeFilter('#cdata', function(nodes) {
      for (var i = 0; i < nodes.length; i++) {
        nodes[i].remove();
      }
    });
  });
}
```

Acknowledgements

Tiny Technologies would like to thank Michał Bentkowski and intivesec for discovering these vulnerabilities.

References

https://www.tiny.cloud/docs/release-notes/release-notes522/#securityfixes

For more information

If you have any questions or comments about this advisory:

- Open an issue in the TinyMCE repo
- Email us at infosec@tiny.cloud

References

- GHSA-c78w-2gw7-gjv3

CVE-2019-20503 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Current Description

usrsctp before 2019-12-20 has out-of-bounds reads in sctp_load_addresses_from_init.

Source: MITRE

View Analysis Description

Severity

CVSS Version 3.x | CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NIST: NVD **Base Score:** 6.5 MEDIUM **Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

Weakness Enumeration

CWE-ID	CWE Name	Source
CWE-125	Out-of-bounds Read	NIST

Known Affected Software Configurations Switch to CPE 2.2

Configuration 1 (hide)

cpe:2.3:a:usrsctp_project:usrsctp:*:*:*:*:*:*:*:*	**Up to (excluding)**
Show Matching CPE(s)	**2019-12-20**

Repositories 1
Code 3K
Commits 39K
Issues 3
Discussions Beta 0
Packages 0
Marketplace 0
Topics 0
Wikis 0
Users 0

Advanced search Cheat sheet

39,032 commit results

Sort: Best match

exthmui-devices/android_kernel_xiaomi_sdm845 97b89f3
Merge branch 'android-4.9-q' of https://android.googlesource.com/kern…
bgcngm committed on 24 Apr

exthmui-devices/android_kernel_xiaomi_dipper 97b89f3
Merge branch 'android-4.9-q' of https://android.googlesource.com/kern…
bgcngm committed on 24 Apr

milouk/Sphinx-Beryllium 97b89f3
Merge branch 'android-4.9-q' of https://android.googlesource.com/kern…
bgcngm committed on 24 Apr

LineageOS/android_kernel_xiaomi_sdm845 97b89f3
Merge branch 'android-4.9-q' of https://android.googlesource.com/kern…
bgcngm committed on 24 Apr

dinosnore1/lumos_beryllium 97b89f3
Merge branch 'android-4.9-q' of https://android.googlesource.com/kern…
bgcngm committed on 24 Apr

PixelExperience-Devices/kernel_xiaomi_dipper 97b89f3
Merge branch 'android-4.9-q' of https://android.googlesource.com/kern…
bgcngm committed on 24 Apr

AICP/kernel_xiaomi_sdm845 97b89f3
Merge branch 'android-4.9-q' of https://android.googlesource.com/kern…
bgcngm committed on 24 Apr

Sony-MSM8994-Dev/android_kernel_sony_msm8994 30f5603
Merge tag 'v3.10.106' into lineage-15.1
rk779 authored and **TARKZiM** committed on 10 Jul 2018

yudiwdynto/msm-4.14 f98738c
Merge tag 'v4.14.161' into kernel.lnx.4.14.r11-rel
yudiwdynto committed on 16 May

rico192/kernel_xiaomi_rosy Verified 2a91965
Merge branch 'linux-3.18.y' of https://kernel.googlesource.com/pub/sc…
mscalindt committed on 19 Apr

CVE-2020-9489 Detail

Current Description

A carefully crafted or corrupt file may trigger a System.exit in Tika's OneNote Parser. Crafted or corrupted files can also cause out of memory errors and/or infinite loops in Tika's ICNSParser, MP3Parser, MP4Parser, SAS7BDATParser, OneNoteParser and ImageParser. Apache Tika users should upgrade to 1.24.1 or later. The vulnerabilities in the MP4Parser were partially fixed by upgrading the com.googlecode:isoparser:1.1.22 dependency to org.tallison:isoparser:1.9.41.2. For unrelated security reasons, we upgraded org.apache.cxf to 3.3.6 as part of the 1.24.1 release.

Source: MITRE

+View Analysis Description

Severity

CVSS Version 3.x | CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NIST: NVD **Base Score:** 5.5 MEDIUM **Vector:** CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

Hyperlink	Resource
https://lists.apache.org/thread.html/r4d943777e36ca3aa6305a45da5acccc54ad894f2d5a07186cfa2442c%40%3Cdev.tika.apache.org%3E	Mailing List Vendor Advisory

Weakness Enumeration

CWE-ID	CWE Name	Source
CWE-401	Missing Release of Memory after Effective Lifetime	NIST

Known Affected Software Configurations Switch to CPE 2.2

Configuration 1 (hide)

cpe:2.3:a:apache:tika:1.24:*:*:*:*:*:*:*

Hide Matching CPE(s)

- *cpe:2.3:a:apache:tika:1.24:*:*:*:*:*:*:**

CVE-2019-9948 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Current Description

urllib in Python 2.x through 2.7.16 supports the local_file: scheme, which makes it easier for remote attackers to bypass protection mechanisms that blacklist file: URIs, as demonstrated by triggering a urllib.urlopen('local_file:///etc/passwd') call.

Source: MITRE

View Analysis Description

Severity

CVSS Version 3.x | CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NIST: NVD **Base Score:** 9.1 CRITICAL **Vector:** CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

Weakness Enumeration

CWE-ID	CWE Name	Source
CWE-254	7PK - Security Features	NIST

Known Affected Software Configurations Switch to CPE 2.2

Configuration 1 (hide)

cpe:2.3:a:python:python:*:*:*:*:*:*:*:*	From (including)	Up to (including)
Show Matching CPE(s)	2.0	2.7.15
cpe:2.3:a:python:python:2.7.16:-:*:*:*:*:*:*		
Show Matching CPE(s)		

Configuration 2 (hide)

cpe:2.3:o:opensuse:leap:15.0:*:*:*:*:*:*:*
Show Matching CPE(s)

Configuration 3 (hide)

cpe:2.3:a:netapp:active_iq_performance_analytics_services:-:*:*:*:*:*:*:*
Show Matching CPE(s)

Select all items matching search query

CVE	Application	Version	CVE description	CPE
CVE-2018-17182		-	An issue was discovered in the Linux kernel through 4.18.8. The vmacache_flush_all function in mm/vmacache.c mishandles sequence number overflows. An attacker can trigger a use-after-free (and possibly gain privileges) via certain thread creation, map, unmap, invalidation, and dereference operations.	a:netapp:active_iq_performance_analytics_services:*:*:*:*:*:*:*:*
CVE-2018-12099		-	Grafana before 5.2.0-beta1 has XSS vulnerabilities in dashboard links.	a:netapp:active_iq_performance_analytics_services:*:*:*:*:*:*:*:*
CVE-2018-14634		-	An integer overflow flaw was found in the Linux kernel's create_elf_tables() function. An unprivileged local user with access to SUID (or otherwise privileged) binary could use this flaw to escalate their privileges on the system. Kernel versions 2.6.x, 3.10.x and 4.14.x are believed to be vulnerable.	a:netapp:active_iq_performance_analytics_services:*:*:*:*:*:*:*:*
			An issue was discovered in the Linux	

jeremylong / DependencyCheck

Watch 117 | Star 2.4k | Fork 635

Code | Issues 257 | Pull requests 1 | Actions | Wiki | Security | Insights

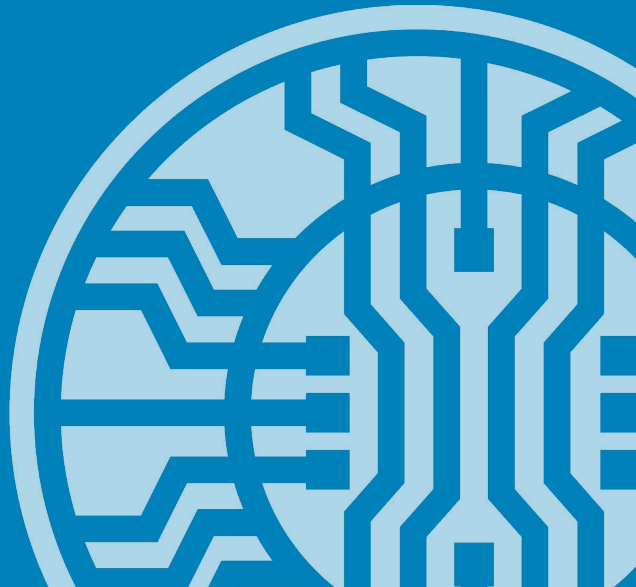
is:issue is:open

Labels 21 | Milestones 1 | New issue

257 Open | 1,550 Closed | Author | Label | Projects | Milestones | Assignee | Sort

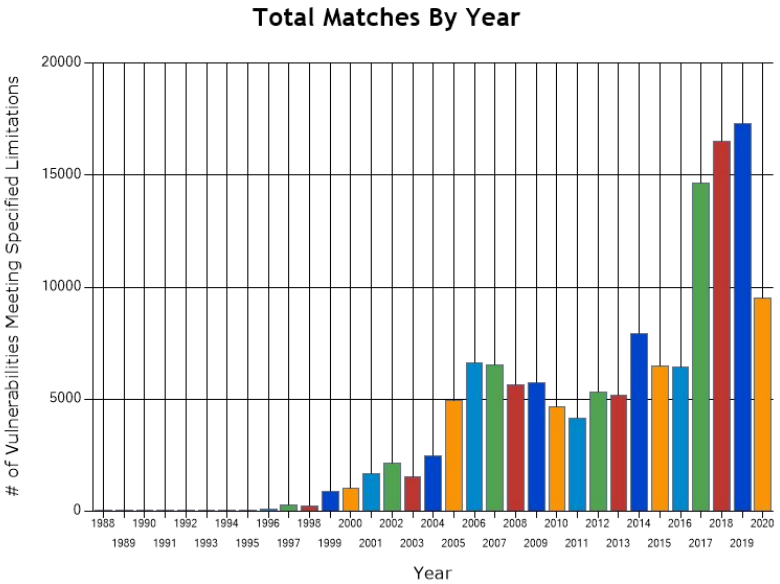
- **False Positive on cachecontrol_2.12-2.0.0.jar** FP Report
  #2683 opened 3 hours ago by sathish-kumar-subramani
- **Golang Mod Analyzer: Reason for using go mod edit -json** question
  #2680 opened yesterday by PurriateCat
- **False Positive on camel-cxf** FP Report
  #2678 opened 3 days ago by rwalravens
- **False Positive on elastic-apm-agent** FP Report
  #2676 opened 6 days ago by OrangeDog
- **False Positive on geronimo-health-1.0.2** FP Report
  #2673 opened 8 days ago by fpapon
- **False Positive on geronimo-metrics-1.0.4** FP Report
  #2672 opened 8 days ago by fpapon
- **Customizing data directory and cveUrl's, execution fails the first two times** question
  #2670 opened 9 days ago by twh270
- **jenkins plugin:** question
  #2669 opened 13 days ago by cigfthomas
- **vulnerabilityIdMatched inconsistent between multiple runs** bug — 1
  #2665 opened 15 days ago by RyanMcC
- **What is the correct syntax for enabling python analyzer on jenkins** question — 2
  #2663 opened 18 days ago by anshbansal
- **Reactor dependencies not cought**
  #2662 opened 20 days ago by mbenz89
- **How do I scan my iOS Swift repository which contains Podfile.lock and Package.resolved files?** question — 2
  #2660 opened 21 days ago by SubParDev
- **jenkins plugin : publishing several reports at once has strange behavior** bug — 1
  #2658 opened 23 days ago by aubertaa
- **False Positive on gradle** FP Report
  #2657 opened 24 days ago by tmyroadctfig
- **False Positive on jasperreports-6.8.1.jar (pkg:maven/net.sf.jasperreports/jasperreports@6.8.1)** FP Report
  #2652 opened on 25 May by KuzinGit
- **False Positive on pkg:maven/com.vaadin/vaadin-testbench-core@6.3.0.beta1** FP Report
  #2651 opened on 25 May by ZheSun88
- **False Positive on pkg:maven/org.sonatype.nexus.plugins/nexus-restore-helm@1.0.5** FP Report
  #2650 opened on 20 May by wagdez

This is bad … how to solve it?



Data Quality

- 350 CVE / week
- Throwing machine at garbage data will produce garbage output … might help at pointing out inconsistencies
- Manual vetting of data

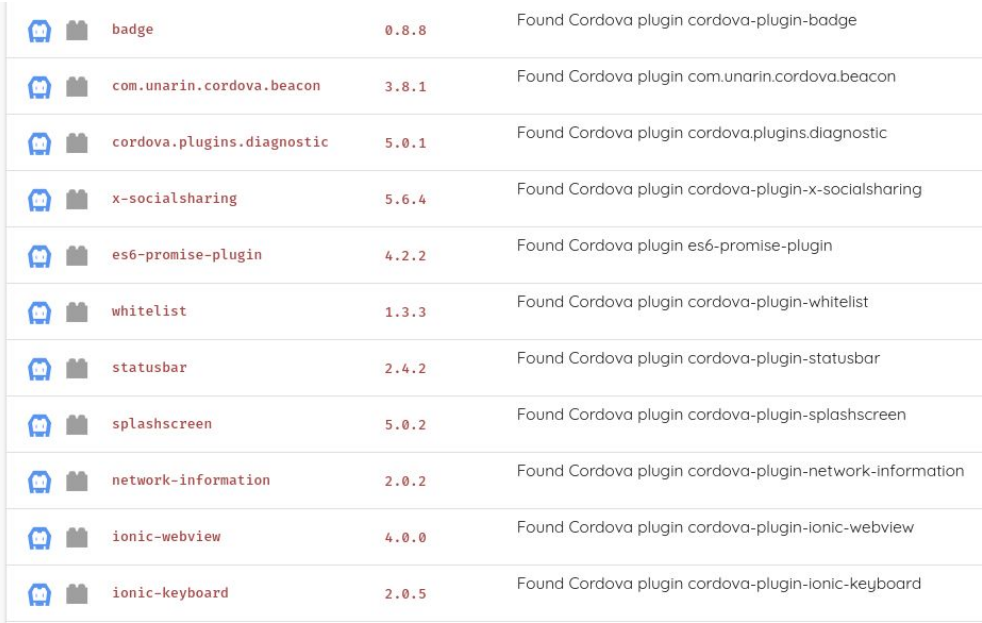


Identification

	Coverage	Complexity	Source Code	Transitive dependencies	Embedded dependencies
OS	OS only	Simple	Not required	Very limited	No
Package Manager	Open source packages only	Simple	Required	Good	No
Fingerprint	All	Complex	Not required	Great	Yes

Shallow Fingerprinting

- **iOS:** Frameworks Plist files
- **Cordova:** cordova_plugins.js
- **React:** javascript bundle file
- **Native:** BuildConfig Application ID
- ...

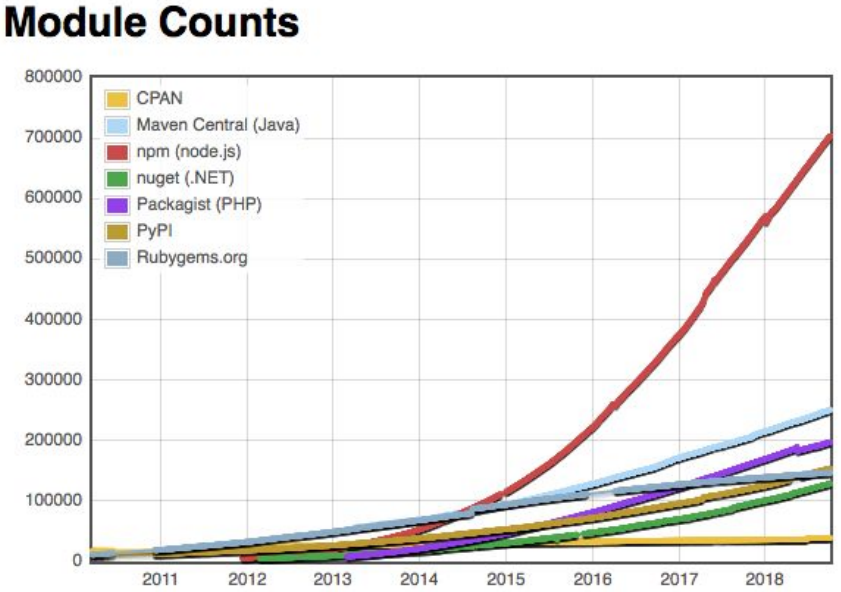


Shallow Fingerprinting

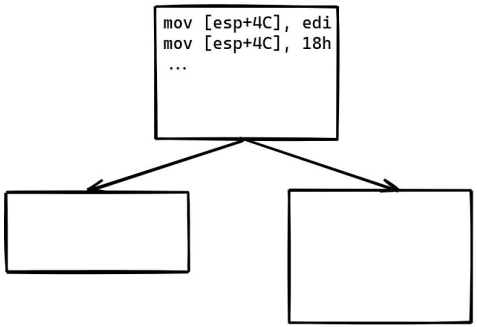
mocha	7.0.0
mkdirp	latest
express	latest
del	latest
code-push-plugin-testing-framework	file:./code-push-plugin-testing-framework

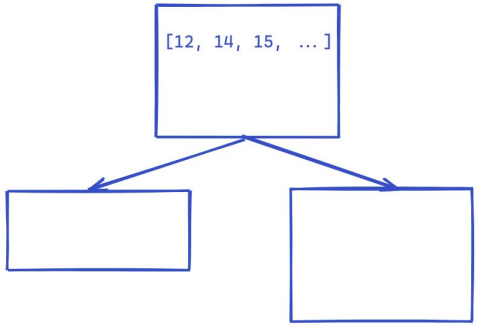
Deep Fingerprinting

- Extraction of features from binaries to uniquely identify vulnerable versions
- CFG, strings, N-grams, package names, metadata, AST ...
- **15M+** Jar and AAR on several Maven repositories
- **70k+** Cocoapod
- ...

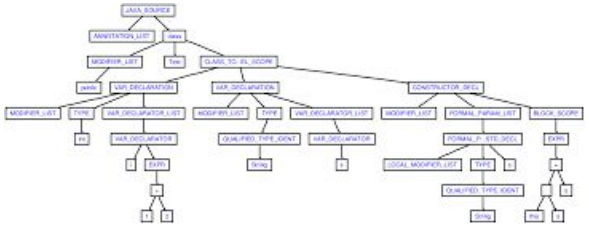


Deep Fingerprinting






```
1 .class public Ltvi/webrtc/AudioSource;
2 .super Ltvi/webrtc/MediaSource;
3 .source "AudioSource.java"
4
```



```
@@ -56,6 +56,12 @@ var _REGEX_STRING = '(<%%|%%>|<%=|<%-|<%_|<%#|<%|%>|-%>|_%>)';
  var _OPTS = [ 'cache', 'filename', 'delimiter', 'scope', 'context',
         'debug', 'compileDebug', 'client', '_with', 'root', 'rmWhitespace',
         'strict', 'localsName'];
+var _OPTS_IN_DATA_BLACKLIST = {
+      cache: true,
+      filename: true,
+      root: true,
+      localsName: true
+    };
  var _BOM = /^\uFEFF/;

  /**
@@ -268,11 +274,9 @@ function rethrow(err, str, filename, lineno){
  function cpOptsInData(data, opts) {
    _OPTS.forEach(function (p) {
      if (typeof data[p] != 'undefined') {
-       // Disallow setting the root opt for includes via a passed data obj
-       // Unsanitized, parameterized use of `render` could allow the
-       // include directory to be reset, opening up the possibility of
-       // remote code execution
-       if (p == 'root') {
+       // Disallow passing potentially dangerous opts in the data
+       // These opts should not be settable via a `render` call
+       if (_OPTS_IN_DATA_BLACKLIST[p]) {
          return;
        }
        opts[p] = data[p];
```

Final notes ...

- 3rd Party Security is not a solved problem
- Out current tools to identify these issues are limited
- Deep & Shallow fingerprinting


Q&A