DEPENDENCY-CHECK

Dependency-Check is an open source tool performing a best effort analysis of 3rd party dependencies; false positives and false negatives may exist in the analysis performed by the tool. Use of the tool and the reporting provided constitutes acceptance for use in an AS IS condition, and there are NO warranties, implied or otherwise, with regard to the analysis or its use. Any use of the tool and the reporting provided is at the user's risk. In no event shall the copyright holder or OWASP be held liable for any damages whatsoever arising out of or in connection with the use of this tool, the analysis performed, or the resulting report.

How to read the report | **Suppressing false positives** | Getting Help: **github issues**

♡ **Sponsor**

Project: SkyFi-ATAK-Plugin-v2

Scan Information ():
- *dependency-check version*: 8.0.2
- *Report Generated On*: Wed, 6 Aug 2025 23:17:53 GMT
- *Dependencies Scanned*: 66 (21 unique)
- *Vulnerable Dependencies*: 2
- *Vulnerabilities Found*: 12
- *Vulnerabilities Suppressed*: 0
- *NVD CVE Checked*: 2025-08-06T23:17:11
- *NVD CVE Modified*: 2025-08-06T22:00:01
- *VersionCheckOn*: 2023-05-15T20:34:10
- *kev.checked*: 1754522249

Summary

Display:

Dependency	Vulnerability IDs	Package	Highest Severity	CVE Count	Confidence	Evidence Count
ATAK-Plugin-SkyFi-ATAK-Plugin-v2-2.0--5.4.0-civ-release.apk				0		2
ATAKPluginTests-debug.aar				0		8
ATAKPluginTests-javadoc.jar				0		2
R.jar				0		3
androidsvg-1.2.1.jar	cpe:2.3:a:androidsvg_project:androidsvg:1.2.1:*:*:*:*:*:*:*	pkg:maven/com.caverock/androidsvg@1.2.1	HIGH	1	Highest	25
atak-gradle-takdev.jar	cpe:2.3:a:gradle:gradle:3.5.3:*:*:*:*:*:*:*		CRITICAL	11	Low	9
atak-javadoc.jar				0		2
base.jar				0		2
gradle-wrapper.jar				0		8
gradle-wrapper.jar				0		8
gradle-wrapper.jar				0		6
main.jar (shaded: ch.acra:acra:4.6.1)		pkg:maven/ch.acra/acra@4.6.1		0		13
main.jar (shaded: com.healthmarketscience.jackcess:jackcess:1.2.14.3)		pkg:maven/com.healthmarketscience.jackcess/jackcess@1.2.14.3		0		28
main.jar				0		3
menu.xml.jar				0		2
plugin.xml.jar				0		2
shrunkJavaRes.jar				0		2
skyfi.xml.jar				0		2
skyfi_logo.png.jar				0		2
takdevlint.aar	cpe:2.3:a:archive_project:archive:3.3.0:snapshot:*:*:*:*:*			0	Low	75
takdevlint.aar: lint.jar				0		7

Dependencies

ATAK-Plugin-SkyFi-ATAK-Plugin-v2-2.0--5.4.0-civ-release.apk

File Path: /app/plugin-src/SkyFi-ATAK-Plugin-v2/app/build/outputs/apk/civ/release/ATAK-Plugin-SkyFi-ATAK-Plugin-v2-2.0--5.4.0-civ-release.apk
MD5: 7287a3003427bb74f58af211760619da
SHA1: e9c79450edf1975e9ea86ce4047161204e18447e
SHA256: eb10c6e35aae7c0a57c5a9973c3f998bdf3bfaa2cd75988622bab1bf231be93b

> Evidence

> Identifiers
>> - **None**

ATAKPluginTests-debug.aar

File Path: /app/plugin-src/SkyFi-ATAK-Plugin-v2/sdk/ATAK-CIV-5.4.0.18-SDK/espresso/ATAKPluginTests-debug.aar
MD5: c035fe8ce16372293f50f5ca5d9d3093
SHA1: 106c58d16337849b6f36d091445b5127337e1f87
SHA256: 14bfa3a506e0549aab63e87dc230e7be2f19b515ef5d034b5088cf5c324f238e

> Evidence

Related Dependencies

Identifiers

- **None**

ATAKPluginTests-javadoc.jar

File Path: /app/plugin-src/SkyFi-ATAK-Plugin-v2/sdk/ATAK-CIV-5.4.0.18-SDK/espresso/ATAKPluginTests-javadoc.jar
MD5: 58c69c5891d8341e227823d6e4591360
SHA1: 1b1f0b0c2521660fc258e809bd5fb5f45f1a42db
SHA256: 156d2fee7b3dea178d4281a36e96ef15186e398c73cb776f075471e264188910

Evidence

Identifiers

- **None**

R.jar

File Path: /app/plugin-src/SkyFi-ATAK-Plugin-v2/app/build/intermediates/compile_and_runtime_not_namespaced_r_class_jar/civRelease/R.jar
MD5: c5db000250c400f995cbdf97ad387040
SHA1: bc72c58290069b973a0191658849e46b4b92c257
SHA256: ce310e4b9d17bde7f70db1d12df597d12632f85b42deee36558dee1ec942d94f

Evidence

Identifiers

- **None**

---

androidsvg-1.2.1.jar

Description:

AndroidSVG is an SVG rendering library for Android.

License:

The Apache Software License, Version 2.0: http://www.apache.org/licenses/LICENSE-2.0.txt

File Path: /app/plugin-src/SkyFi-ATAK-Plugin-v2/sdk/ATAK-CIV-5.4.0.18-SDK/samples/hello3d/app/libs/androidsvg-1.2.1.jar
MD5: f091fe8be4d04981121aae8d77542757
SHA1: d0cb3453e18fffeb053e9b7f052af3dcec9f75b4
SHA256: 3233718b83f2ca778597bdd3705ee2eb23fa0e22e236f78f48854f7a0c27c3d5

Evidence

Related Dependencies

Identifiers

- pkg:maven/com.caverock/androidsvg@1.2.1 (*Confidence*:High)
- cpe:2.3:a:androidsvg_project:androidsvg:1.2.1:*:*:*:*:*:*:* (*Confidence*:Highest) suppress

Published Vulnerabilities

CVE-2017-1000498 (OSSINDEX) suppress

AndroidSVG version 1.2.2 is vulnerable to XXE attacks in the SVG parsing component resulting in denial of service and possibly remote code execution

CWE-611 Improper Restriction of XML External Entity Reference ('XXE')

CVSSv2:
- Base Score: HIGH (7.8)
- Vector: /AV:L/AC:L/Au:/C:H/I:H/A:H

References:
- OSSINDEX - [CVE-2017-1000498] CWE-611: Improper Restriction of XML External Entity Reference ('XXE')
- OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-1000498
- OSSIndex - https://github.com/BigBadaboom/androidsvg/issues/122

Vulnerable Software & Versions (OSSINDEX):

- cpe:2.3:a:com.caverock:androidsvg:1.2.1:*:*:*:*:*:*:*

---

atak-gradle-takdev.jar

File Path: /app/plugin-src/SkyFi-ATAK-Plugin-v2/atak-gradle-takdev.jar
MD5: 6bd5002e13c43be0f1c137ffa41ee11a
SHA1: a2f75db9ab0324c2d1b64cb879db56b24fcf4fcb

Evidence

Related Dependencies

Identifiers

- cpe:2.3:a:gradle:gradle:3.5.3:*:*:*:*:*:*:* (*Confidence*:Low) suppress

Published Vulnerabilities

CVE-2019-15052 suppress

The HTTP client in Gradle before 5.6 sends authentication credentials originally destined for the configured host. If that host returns a 30x redirect, Gradle also sends those credentials to all subsequent hosts that the request redirects to. This is similar to CVE-2018-1000007.

CWE-522 Insufficiently Protected Credentials

CVSSv2:
- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:P/I:N/A:N

CVSSv3:
- Base Score: CRITICAL (9.8)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

References:
- - https://github.com/gradle/gradle/issues/10278
- - https://github.com/gradle/gradle/pull/10176
- - https://github.com/gradle/gradle/security/advisories/GHSA-4cwg-f7qc-6r95

Vulnerable Software & Versions:
- cpe:2.3:a:gradle:gradle:*:*:*:*:*:*:*:* versions up to (excluding) 5.6

CVE-2023-35947 suppress

Gradle is a build tool with a focus on build automation and support for multi-language development. In affected versions when unpacking Tar archives, Gradle did not check that files could be written outside of the unpack location. This could lead to important files being overwritten anywhere the Gradle process has write permissions. For a build reading Tar entries from a Tar archive, this issue could allow Gradle to disclose information from sensitive files through an arbitrary file read. To exploit this behavior, an attacker needs to either control the source of an archive already used by the build or modify the build to interact with a malicious archive. It is unlikely that this would go unnoticed. A fix has been released in Gradle 7.6.2 and 8.2 to protect against this vulnerability. Starting from these versions, Gradle will refuse to handle Tar archives which contain path traversal elements in a Tar entry name. Users are advised to upgrade. There are no known workarounds for this vulnerability.

Impact

This is a path traversal vulnerability when Gradle deals with Tar archives, often referenced as TarSlip, a variant of ZipSlip.

* When unpacking Tar archives, Gradle did not check that files could be written outside of the unpack location. This could lead to important files being overwritten anywhere the Gradle process has write permissions.
* For a build reading Tar entries from a Tar archive, this issue could allow Gradle to disclose information from sensitive files through an arbitrary file read.

To exploit this behavior, an attacker needs to either control the source of an archive already used by the build or modify the build to interact with a malicious archive. It is unlikely that this would go unnoticed.

Gradle uses Tar archives for its [Build Cache](https://docs.gradle.org/current/userguide/build_cache.html). These archives are safe when created by Gradle. But if an attacker had control of a remote build cache server, they could inject malicious build cache entries that leverage this vulnerability. This attack vector could also be exploited if a man-in-the-middle can be performed between the remote cache and the build.

Patches

A fix has been released in Gradle 7.6.2 and 8.2 to protect against this vulnerability. Starting from these versions, Gradle will refuse to handle Tar archives which contain path traversal elements in a Tar entry name.

It is recommended that users upgrade to a patched version.

Workarounds

There is no workaround.

* If your build deals with Tar archives that you do not fully trust, you need to inspect them to confirm they do not attempt to leverage this vulnerability.
* If you use the Gradle remote build cache, make sure only trusted parties have write access to it and that connections to the remote cache are properly secured.

References

* [CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')](https://cwe.mitre.org/data/definitions/22.html)
* [Gradle Build Cache](https://docs.gradle.org/current/userguide/build_cache.html)
* [ZipSlip](https://security.snyk.io/research/zip-slip-vulnerability)

CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

CVSSv3:
- Base Score: HIGH (8.1)
- Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

References:
- - https://github.com/gradle/gradle/commit/1096b309520a8c315e3b6109a6526de4eabcb879
- - https://github.com/gradle/gradle/commit/2e5c34d57d0c0b7f0e8b039a192b91e5c8249d91
- - https://github.com/gradle/gradle/security/advisories/GHSA-84mw-qh6q-v842
- - https://security.netapp.com/advisory/ntap-20230803-0007/

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gradle:gradle:*:*:*:*:*:*:*:* versions up to (excluding) 7.6.2
- ...

CVE-2021-29428 suppress

In Gradle before version 7.0, on Unix-like systems, the system temporary directory can be created with open permissions that allow multiple users to create and delete files within it. Gradle builds could be vulnerable to a local privilege escalation from an attacker quickly deleting and recreating files in the system temporary directory. This vulnerability impacted builds using precompiled script plugins written in Kotlin DSL and tests for Gradle plugins written using ProjectBuilder or TestKit. If you are on Windows or modern versions of macOS, you are not vulnerable. If you are on a Unix-like operating system with the "sticky" bit set on your system temporary directory, you are not vulnerable. The problem has been patched and released with Gradle 7.0. As a workaround, on Unix-like operating systems, ensure that the "sticky" bit is set. This only allows the original user (or root) to delete a file. If you are unable to change the permissions of the system temporary directory, you can move the Java temporary directory by setting the System Property `java.io.tmpdir`. The new path needs to limit permissions to the build user only. For additional details refer to the referenced GitHub Security Advisory.

CVSSv2:
- Base Score: MEDIUM (4.4)
- Vector: /AV:L/AC:M/Au:N/C:P/I:P/A:P

CVSSv3:
- Base Score: HIGH (7.8)
- Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

References:
- - https://docs.gradle.org/7.0/release-notes.html#security-advisories

- - https://github.com/gradle/gradle/pull/15240
  - - https://github.com/gradle/gradle/pull/15654
  - - https://github.com/gradle/gradle/security/advisories/GHSA-89qm-pxvm-p336

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gradle:gradle:*:*:*:*:*:*:*:* versions up to (excluding) 7.0
- ...

CVE-2020-11979 `suppress`

As mitigation for CVE-2020-1945 Apache Ant 1.10.8 changed the permissions of temporary files it created so that only the current user was allowed to access them. Unfortunately the fixcrlf task deleted the temporary file and created a new one without said protection, effectively nullifying the effort. This would still allow an attacker to inject modified source files into the build process.

NVD-CWE-Other

CVSSv2:
- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:N/I:P/A:N

CVSSv3:
- Base Score: HIGH (7.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

References:
- - FEDORA-2020-2640aa4e19
- - FEDORA-2020-3ce0f55bc5
- - FEDORA-2020-92b1d001b3
- - GLSA-202011-18
- - [creadur-dev] 20201006 [jira] [Assigned] (RAT-274) Update to at least Ant 1.10.8/1.9.15 in order to fix CVE-2020-11979
- - [creadur-dev] 20201006 [jira] [Commented] (RAT-274) Update to at least Ant 1.10.8/1.9.15 in order to fix CVE-2020-11979
- - [creadur-dev] 20201006 [jira] [Resolved] (RAT-274) Update to at least Ant 1.10.8/1.9.15 in order to fix CVE-2020-11979 / raise compiler level to JDK8
- - [creadur-dev] 20201006 [jira] [Updated] (RAT-274) Update to at least Ant 1.10.8/1.9.15 in order to fix CVE-2020-11979
- - [creadur-dev] 20201006 [jira] [Updated] (RAT-274) Update to at least Ant 1.10.8/1.9.15 in order to fix CVE-2020-11979 / raise compiler level to JDK8
- - [creadur-dev] 20210419 [jira] [Commented] (RAT-274) Update to at least Ant 1.10.8/1.9.15 in order to fix CVE-2020-11979 / raise compiler level to JDK8
- - [creadur-dev] 20210621 [jira] [Commented] (RAT-274) Update to at least Ant 1.10.8/1.9.15 in order to fix CVE-2020-11979 / raise compiler level to JDK8
- - https://github.com/gradle/gradle/security/advisories/GHSA-j45w-qrgf-25vm
- - https://lists.apache.org/thread.html/rc3c8ef9724b5b1e171529b47f4b35cb7920edfb6e917fa21eb6c64ea%40%3Cdev.ant.apache.org%3E
- - https://www.oracle.com//security-alerts/cpujul2021.html
- - https://www.oracle.com/security-alerts/cpuApr2021.html
- - https://www.oracle.com/security-alerts/cpuapr2022.html
- - https://www.oracle.com/security-alerts/cpujan2021.html
- - https://www.oracle.com/security-alerts/cpujan2022.html
- - https://www.oracle.com/security-alerts/cpuoct2021.html

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gradle:gradle:*:*:*:*:*:*:*:* versions up to (excluding) 6.8.0
- ...

CVE-2021-32751 `suppress`

Gradle is a build tool with a focus on build automation. In versions prior to 7.2, start scripts generated by the `application` plugin and the `gradlew` script are both vulnerable to arbitrary code execution when an attacker is able to change environment variables for the user running the script. This may impact those who use `gradlew` on Unix-like systems or use the scripts generated by Gradle in thieir application on Unix-like systems. For this vulnerability to be exploitable, an attacker needs to be able to set the value of particular environment variables and have those environment variables be seen by the vulnerable scripts. This issue has been patched in Gradle 7.2 by removing the use of `eval` and requiring the use of the `bash` shell. There are a few workarounds available. For CI/CD systems using the Gradle build tool, one may ensure that untrusted users are unable to change environment variables for the user that executes `gradlew`. If one is unable to upgrade to Gradle 7.2, one may generate a new `gradlew` script with Gradle 7.2 and use it for older versions of Gradle. Fpplications using start scripts generated by Gradle, one may ensure that untrusted users are unable to change environment variables for the user that executes the start script. A vulnerable start script could be manually patched to remove the use of `eval` or the use of environment variables that affect the application's command-line. If the application is simple enough, one may be able to avoid the use of the start scripts by running the application directly with Java command.

CWE-78 Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

CVSSv2:
- Base Score: HIGH (8.5)
- Vector: /AV:N/AC:M/Au:S/C:C/I:C/A:C

CVSSv3:
- Base Score: HIGH (7.5)
- Vector: CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H

References:
- - https://github.com/gradle/gradle/security/advisories/GHSA-6j2p-252f-7mw8
- - https://medium.com/dot-debug/the-perils-of-bash-eval-cc5f9e309cae
- - https://mywiki.wooledge.org/BashFAQ/048

Vulnerable Software & Versions:

- cpe:2.3:a:gradle:gradle:*:*:*:*:*:*:*:* versions up to (excluding) 7.2

CVE-2023-44387 `suppress`

Gradle is a build tool with a focus on build automation and support for multi-language development. When copying or archiving symlinked files, Gradle resolves them but applies the permissions of the symlink itself instead of the permissions of the linked file to the resulting file. This leads to files having too much permissions given that symlinks usually are world readable and writeable. While it is unlikely this results in a direct vulnerability for the impacted build, it may open up attack vectors depending on where build artifacts end up being copied to or un-archived. In versions 7.6.3, 8.4 and above, Gradle will now properly use the permissions of the file pointed at by the symlink to set permissions of the copied or archived file.

CVSSv3:
- Base Score: MEDIUM (6.5)
- Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N

References:
- - https://github.com/gradle/gradle/commit/3b406191e24d69e7e42dc3f3b5cc50625aa930b7
- - https://github.com/gradle/gradle/releases/tag/v7.6.3
- - https://github.com/gradle/gradle/releases/tag/v8.4.0
- - https://github.com/gradle/gradle/security/advisories/GHSA-43r3-pqhv-f7h9
- - https://security.netapp.com/advisory/ntap-20231110-0006/

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gradle:gradle:*:*:*:*:*:*:*:* versions up to (excluding) 7.6.3
- ...

CVE-2019-11065 `suppress`

Gradle versions from 1.4 to 5.3.1 use an insecure HTTP URL to download dependencies when the built-in JavaScript or CoffeeScript Gradle plugins are used. Dependency artifacts could have been maliciously compromised by a MITM attack against the ajax.googleapis.com web site.

NVD-CWE-noinfo

CVSSv2:
- Base Score: MEDIUM (4.3)
- Vector: /AV:N/AC:M/Au:N/C:P/I:N/A:N

CVSSv3:
- Base Score: MEDIUM (5.9)
- Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N

References:
- - FEDORA-2019-1b6383acdd
- - FEDORA-2019-902786bc1e
- - FEDORA-2019-a9c15101fb
- - https://github.com/gradle/gradle/pull/8927

Vulnerable Software & Versions:

- cpe:2.3:a:gradle:gradle:*:*:*:*:*:*:*:* versions from (including) 1.4; versions up to (including) 5.3.1

CVE-2019-16370 `suppress`

The PGP signing plugin in Gradle before 6.0 relies on the SHA-1 algorithm, which might allow an attacker to replace an artifact with a different one that has the same SHA-1 message digest, a related issue to CVE-2005-4900.

CWE-327 Use of a Broken or Risky Cryptographic Algorithm

CVSSv2:
- Base Score: MEDIUM (4.3)
- Vector: /AV:N/AC:M/Au:N/C:N/I:P/A:N

CVSSv3:
- Base Score: MEDIUM (5.9)
- Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N

References:
- - https://github.com/gradle/gradle/commit/425b2b7a50cd84106a77cdf1ab665c89c6b14d2f
- - https://github.com/gradle/gradle/pull/10543

Vulnerable Software & Versions:

- cpe:2.3:a:gradle:gradle:*:*:*:*:*:*:*:* versions up to (excluding) 6.0

CVE-2021-29429 `suppress`

In Gradle before version 7.0, files created with open permissions in the system temporary directory can allow an attacker to access information downloaded by Gradle. Some builds could be vulnerable to a local information disclosure. Remote files accessed through TextResourceFactory are downloaded into the system temporary directory first. Sensitive information contained in these files can be exposed to other local users on the same system. If you do not use the `TextResourceFactory` API, you are not vulnerable. As of Gradle 7.0, uses of the system temporary directory have been moved to the Gradle User Home directory. By default, this directory is restricted to the user running the build. As a workaround, set a more restrictive umask that removes read access to other users. When files are created in the system temporary directory, they will not be accessible to other users. If you are unable to change your system's umask, you can move the Java temporary directory by setting the System Property `java.io.tmpdir`. The new path needs to limit permissions to the build user only.

CVSSv2:
- Base Score: LOW (1.9)
- Vector: /AV:L/AC:M/Au:N/C:P/I:N/A:N

CVSSv3:
- Base Score: MEDIUM (5.5)
- Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N

References:
- - https://docs.gradle.org/7.0/release-notes.html#security-advisories
- - https://github.com/gradle/gradle/security/advisories/GHSA-fp8h-qmr5-j4c8

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gradle:gradle:*:*:*:*:*:*:*:* versions up to (excluding) 7.0
- ...

CVE-2023-35946 `suppress`

Gradle is a build tool with a focus on build automation and support for multi-language development. When Gradle writes a dependency into its dependency cache, it uses the dependency's coordinates to compute a file location. With specially crafted dependency coordinates, Gradle can be made to write files into an unintended location. The file may be written outside the dependency cache or over another file in the dependency cache. This vulnerability could be used to poison the dependency cache or overwrite important files elsewhere on the filesystem where the Gradle process has write permissions. Exploiting this vulnerability requires an attacker to have control over a dependency repository used by the Gradle build or have the ability to modify the build's configuration. It is unlikely that this would go unnoticed. A fix has been released in Gradle 7.6.2 and 8.2 to protect against this vulnerability. Gradle will refuse to cache dependencies that have path traversal elements in their dependency coordinates. It is recommended that users upgrade to a patched version. If you are unable to upgrade to Gradle 7.6.2 or 8.2, `dependency verification` will make this vulnerability more difficult to exploit.

CVSSv3:
- Base Score: MEDIUM (5.5)
- Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N

References:
- - https://docs.gradle.org/current/userguide/dependency_verification.html
- - https://github.com/gradle/gradle/commit/859eae2b2acf751ae7db3c9ffefe275aa5da0d5d
- - https://github.com/gradle/gradle/commit/b07e528feb3a5ffa66bdcc358549edd73e4c8a12
- - https://github.com/gradle/gradle/security/advisories/GHSA-2h6c-rv6q-494v
- - https://security.netapp.com/advisory/ntap-20230731-0003/

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gradle:gradle:*:*:*:*:*:*:*:* versions up to (excluding) 7.6.2
- ...

CVE-2023-42445 `suppress`

Gradle is a build tool with a focus on build automation and support for multi-language development. In some cases, when Gradle parses XML files, resolving XML external entities is not disabled. Combined with an Out Of Band XXE attack (OOB-XXE), just parsing XML can lead to exfiltration of local text files to a remote server. Gradle parses XML files for several purposes. Most of the time, Gradle parses XML files it generated or were already present locally. Only Ivy XML descriptors and Maven POM files can be fetched from remote repositories and parsed by Gradle. In Gradle 7.6.3 and 8.4, resolving XML external entities has been disabled for all use cases to protect against this vulnerability. Gradle will now refuse to parse XML files that have XML external entities.

CWE-611 Improper Restriction of XML External Entity Reference ('XXE')

CVSSv3:
- Base Score: MEDIUM (5.3)
- Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N

References:
- - https://github.com/gradle/gradle/releases/tag/v7.6.3
- - https://github.com/gradle/gradle/releases/tag/v8.4.0
- - https://github.com/gradle/gradle/security/advisories/GHSA-mrff-q8qj-xvg8
- - https://security.netapp.com/advisory/ntap-20231110-0006/

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gradle:gradle:*:*:*:*:*:*:*:* versions up to (excluding) 7.6.3
- ...

atak-javadoc.jar

File Path: /app/plugin-src/SkyFi-ATAK-Plugin-v2/sdk/ATAK-CIV-5.4.0.18-SDK/atak-javadoc.jar
MD5: d0980697b13a9809c9e432b3a4e4f29e
SHA1: af9daea669403258533ee16c2c20c4c79cfa6328
SHA256: 5f0a82dacf65648841dc40735f8e23a263c81d157175832b8295ebb4cb0d9421

Evidence

Identifiers

- **None**

base.jar

File Path: /app/plugin-src/SkyFi-ATAK-Plugin-v2/app/build/intermediates/merged_java_res/civRelease/base.jar
MD5: 58d56a868cb04f6cd7ac72c08eb71f27
SHA1: 68e77037f95d18ba98b5c3c9298baafa30f4cb03
SHA256: dd1135bc8aff7338ce206479a4bd91693d4d73f147acf0a19c3ed9f691fc2578

> Evidence

> Identifiers

- None

gradle-wrapper.jar

File Path: /app/plugin-src/SkyFi-ATAK-Plugin-v2/gradle/wrapper/gradle-wrapper.jar
MD5: bd2800c24d911ce05e46f6a283bf713b
SHA1: 251364b90b8f139c16eb5d5ce376dfa697cba6cd
SHA256: 91a239400bb638f36a1795d8fdf7939d532cdc7d794d1119b7261aac158b1e60

> Evidence

> Related Dependencies

> Identifiers

- None

gradle-wrapper.jar

File Path: /app/plugin-src/SkyFi-ATAK-Plugin-v2/sdk/ATAK-CIV-5.4.0.18-SDK/gradle/wrapper/gradle-wrapper.jar
MD5: 5f9bb0a10e2f8536e2868c9f2f4fffe3
SHA1: c3c3e995ebcc3fe7fff300a60dccc665d957c0e5
SHA256: 1cef53de8dc192036e7b0cc47584449b0cf570a00d560bfaa6c9eabe06e1fc06

> Evidence

> Related Dependencies

> Identifiers

- None

gradle-wrapper.jar

File Path: /app/plugin-src/SkyFi-ATAK-Plugin-v2/sdk/ATAK-CIV-5.4.0.18-SDK/samples/MetricsApi/gradle/wrapper/gradle-wrapper.jar
MD5: 34e61f332027ce6850d6e3d94402ae8c
SHA1: abf08035a417f807e3d91c559b793ad20f5638ab
SHA256: 2db75c40782f5e8ba1fc278a5574bab070adccb2d21ca5a6e5ed840888448046

> Evidence

> Related Dependencies

> Identifiers

- None

main.jar (shaded: ch.acra:acra:4.6.1)

Description:

Publishes a report of an Android application crash to Google docs (or some other end point).

License:

Apache 2: http://www.apache.org/licenses/LICENSE-2.0.txt

File Path: /app/plugin-src/SkyFi-ATAK-Plugin-v2/sdk/ATAK-CIV-5.4.0.18-SDK/main.jar/META-INF/maven/ch.acra/acra/pom.xml
MD5: 90a97ed18b26b0c5e5eccf4cf60c1d42
SHA1: 0fbf824f3dda94ffcdd5178bc9f3c24a3b037e32
SHA256: e2ad40dcae47e85dfb7a1b607182dfe4be5f23f767ef6bf680c1afec54a25171

> Evidence

Identifiers

- pkg:maven/ch.acra/acra@4.6.1 (*Confidence*:High)

---

main.jar (shaded: com.healthmarketscience.jackcess:jackcess:1.2.14.3)

Description:

A pure Java library for reading from and writing to MS Access databases.

File Path: /app/plugin-src/SkyFi-ATAK-Plugin-v2/sdk/ATAK-CIV-5.4.0.18-SDK/main.jar/META-INF/maven/com.healthmarketscience.jackcess/jackcess/pom.xml
MD5: 4ef79d0bd7b24357fd2a9e1e6fdabadc
SHA1: 09d6c9985353c7672d2c09c5c105c28356af650e
SHA256:4d58bee043e2969e2f067939067d09d6d8ef34d0333fd9579891ebfc34c57a2c

Evidence

Identifiers

- pkg:maven/com.healthmarketscience.jackcess/jackcess@1.2.14.3 (*Confidence*:High)

---

main.jar

File Path: /app/plugin-src/SkyFi-ATAK-Plugin-v2/sdk/ATAK-CIV-5.4.0.18-SDK/main.jar
MD5: 6c400b5d5592c918cc5d48b58e74f625
SHA1: b488b5ca44a4e96dfd57287bb783edd4342231a0
SHA256:ed4ba23c870169a5be52773519d1b38bf25161806d2188b1faadd9425d06bebe

Evidence

Identifiers

- None

---

menu.xml.jar

File Path: /app/plugin-src/SkyFi-ATAK-Plugin-v2/app/build/intermediates/compressed_assets/civRelease/out/assets/menu.xml.jar
MD5: 1eaba93a275d367e253fa5605030c86b
SHA1: 034e1c316d66aa734842a062ae6508094e6974c1
SHA256:93675ae21e98782ea515e2943c08f2c31e3edba1ad032c09295f380c644f7837

Evidence

Identifiers

- None

---

plugin.xml.jar

File Path: /app/plugin-src/SkyFi-ATAK-Plugin-v2/app/build/intermediates/compressed_assets/civRelease/out/assets/plugin.xml.jar
MD5: e42a8e0fcfa05b1e7113010fabf7b233
SHA1: 0a23f0db828d981d61b91ea4fa87d0ce3d0f0d3c
SHA256:f59e19e2a431488c44f3d4b88ae36f5be6fb45382727eab7c112944c4439f36a

Evidence

Identifiers

- None

---

shrunkJavaRes.jar

File Path: /app/plugin-src/SkyFi-ATAK-Plugin-v2/app/build/intermediates/shrunk_java_res/civRelease/shrunkJavaRes.jar
MD5: 5d3e69daa9e74747a9c5ddffdc2cb267
SHA1: 0bb3993664c92e39e9f46bba9abc25d13f9fa929
SHA256:e6be1bb1d2af2b14b202ff9016a45bbfe1dc083e4591457aceb06212c9cf36e4

Evidence

Identifiers

- None

skyfi.xml.jar

File Path: /app/plugin-src/SkyFi-ATAK-Plugin-v2/app/build/intermediates/compressed_assets/civRelease/out/assets/skyfi.xml.jar
MD5: 695f033f8c73ec27378532e39efbb4d1
SHA1: ed54c7f8583ce51f0946c3ced21d4c3d3b6049aa
SHA256: 3edb96785f18c84d1fd639373a4407304c426c52b3f0a50c56b3ed5624da68b8

Evidence

Identifiers

- None

skyfi_logo.png.jar

File Path: /app/plugin-src/SkyFi-ATAK-Plugin-v2/app/build/intermediates/compressed_assets/civRelease/out/assets/skyfi_logo.png.jar
MD5: b1fd418f5c1a35090c2108f3db1d30f2
SHA1: 11409d22d2ab5a0abc88f750757802bc28d3d74f
SHA256: 465c9c77ae7120161ad8464dea5176063699c99a28adb74d6486e828d5a04c91

Evidence

Identifiers

- None

takdevlint.aar

File Path: /app/plugin-src/SkyFi-ATAK-Plugin-v2/.takdev/aars/takdevlint.aar
MD5: e2ecd34cf45c5578dbd1268b263394cd
SHA1: ec3c1922afdf678e5a666bab75ae1da246a95ab1
SHA256: 55673f412db5beae8391e8d58c3e5e10b52807cc33738b470395a08d0766c61e

Evidence

Related Dependencies

Identifiers

- cpe:2.3:a:archive_project:archive:3.3.0:snapshot:*:*:*:*:*:* (*Confidence*:Low) suppress

takdevlint.aar: lint.jar

File Path: /app/plugin-src/SkyFi-ATAK-Plugin-v2/.takdev/aars/takdevlint.aar/lint.jar
MD5: d99111c1379b2c8bf6f2765279f7c985
SHA1: 3d9661af7dbc1b08634ae40ee66dd5bd49758e57
SHA256: e76b2ee0fe07c5da5f6a3ff73e543d11f24f56d085f715732ec4c0bf5ebfd465

Evidence

Related Dependencies

Identifiers

- None