gradle / **gradle** Public

Code · Issues 2k · Pull requests 144 · Actions · Projects 1 · **Security** 10 · ...

Arbitrary code execution via specially crafted environment variables

High **big-guy** published **GHSA-6j2p-252f-7mw8** on Jul 20, 2021

Package

Gradle (Java)

Affected versions	Patched versions
<7.2	7.2

Description

Impact

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 you if you use `gradlew` on Unix-like systems or use the scripts generated by Gradle in your application on Unix-like systems.

For `gradlew`, commands can be included in either `JAVA_OPTS` or `GRADLE_OPTS`.
For start scripts, commands can be included in either `JAVA_OPTS` or `<APP_NAME>_OPTS`.

For example, if a command is added to `JAVA_OPTS` and the user runs a Gradle build:

```
$ export JAVA_OPTS='-Xmx512m $(touch foo)'
$ ./gradlew build
```

This will execute `touch foo`, but any command will work here. When determining the command-line for the Java process that is started by the script, any commands found in these environment variables will be executed as the user running the script.

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 vulnerability was found during a security audit. We do not know of any exploits based on this vulnerability.

Patches

This issue has been patched in Gradle 7.2 by updating our start script template.

Workarounds

CI/CD systems using the Gradle build tool

You are not vulnerable if untrusted users are unable to change environment variables for the user that executes `gradlew`.

If you are unable to upgrade to Gradle 7.2, you can generate a new `gradlew` script with Gradle 7.2 and use it for older versions of Gradle.

Applications using start scripts generated by Gradle

You are not vulnerable if untrusted users are unable to change environment variables for the user that executes the start script.

If you are unsure, the 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, you may be able to avoid the use of the start scripts by running the application directly with Java command.

References

- Eval command and security issues
- The perils of Bash 'eval'

Questions?

- For security related issues, please email us at security@gradle.com.
- For non-security related issues, please open an issue on GitHub.

Severity

High

CVE ID

CVE-2021-32751

Weaknesses

CWE-78