Arbitrary File Write via Archive Extraction (Zip Slip)

Affecting com.diffplug.gradle:goomph package, versions [,3.37.2)

Snyk CVSS

Attack Complexity **High**

Integrity HIGH

See more

INTRODUCED: 16 AUG 2022 CVE-2022-26049
CWE-29

Share

How to fix?

Upgrade `com.diffplug.gradle:goomph` to version 3.37.2 or higher.

Overview

Affected versions of this package are vulnerable to Arbitrary File Write via Archive Extraction (Zip Slip). It allows a malicious zip file to potentially break out of the expected destination directory, writing contents into arbitrary locations on the file system. Overwriting certain files/directories could allow an attacker to achieve remote code execution on a target system by exploiting this vulnerability.

Note: This could have allowed a malicious zip file to extract itself into an arbitrary directory. The only file that Goomph extracts is the p2 bootstrapper and eclipse metadata files hosted at eclipse.org, which are not malicious, so the only way this vulnerability could have affected you is if you had set a custom bootstrap zip, and that zip was malicious.

Details

NVD 8.8 HIGH

It is exploited using a specially crafted zip archive, that holds path traversal filenames. When exploited, a filename in a malicious archive is concatenated to the target extraction directory, which results in the final path ending up outside of the target folder. For instance, a zip may hold a file with a "../../file.exe" location and thus break out of the target folder. If an executable or a configuration file is overwritten with a file containing malicious code, the problem can turn into an arbitrary code execution issue quite easily.

The following is an example of a zip archive with one benign file and one malicious file. Extracting the malicous file will result in traversing out of the target folder, ending up in `/root/.ssh/` overwriting the `authorized_keys` file:

```
+2018-04-15 22:04:29 ..... 19 19 good.txt

+2018-04-15 22:04:42 ..... 20 20
../../../../../../root/.ssh/authorized_keys
```

References

- GitHub Commit
- GitHub Issue

Test your applications

Snyk ID **SNYK-JAVA-COMDIFFPLUGGRADLE-2981040**

Published **16 Aug 2022**

Disclosed **16 Aug 2022**

Credit **Jonathan Leitschuh**

Report a new vulnerability

Found a mistake?

Blog

FAQs

COMPANY

About

Jobs

Contact

Policies

Do Not Sell My Personal Information

CONTACT US

Support

Report a new vuln

Press Kit

Events

FIND US ONLINE

TRACK OUR DEVELOPMENT

DevSecCon

Join the >> community

Registered in England and Wales. Company number: 09677925

Registered address: Highlands House, Basingstoke Road, Spencers Wood, Reading, Berkshire, RG7 1NT.