15

Several simple remote code execution in pdf-image

Share:

TIMELINE

gabriel-kimiaie submitted a report to Node.js third-party modules. Jan 23rd (3 years ago)

I would like to report "A simple remote code execution" in "pdf-image".
It allows "a remote attacker to execute arbitrary code when several functions of the PDFImage class are called and the class loaded from user-input value".

Module

module name: pdf-image
version: latest
npm page: `https://www.npmjs.com/package/pdf-image`

Module Description

Provides an interface to convert PDF's pages to png files in Node.js by using ImageMagick.

Module Stats

[1] weekly downloads: 8,691

Vulnerability

Vulnerability Description

Hello there ! I understand this bug isn't eligible for a bounty. I am reporting it either way. I've found several code execution in the pdf-image class, I tested one of them. They are simple and of course come from the child_process.exec call with lack of escaping. I tested one of them.

Steps To Reproduce:

```
var PDFImage = require("pdf-image").PDFImage;

var pdfImage = new PDFImage('"; sleep 500 #"');
pdfImage.getInfo();
```

You can also exploit the vulnerability by submitting backticks (example payload: `ls;sleep 5` which will be executed even though you're double-quoting the input.

Patch

You can take example on your command-exists npm class:

```
var isUsingWindows = process.platform == 'win32'
var cleanInput = function(s) {
if (/[^A-Za-z0-9_\/:=-]/.test(s)) {
s = "'"+s.replace(/'/g,"'\''")+"'";
s = s.replace(/^(?:'')+/g, '') // unduplicate single-quote at the beginning
.replace(/\'''/g, "\'" ); // remove non-escaped single-quote if there are enclosed between 2 escaped
}
return s;
}

if (isUsingWindows) {
cleanInput = function(s) {
var isPathName = /[\]/.test(s);
if (isPathName) {
var dirname = '"' + path.dirname(s) + '"';
var basename = '"' + path.basename(s) + '"';
return dirname + ':' + basename;
}
return '"' + s + '"';
}
}
```

Supporting Material/References:

https://github.com/mooz/node-pdf-image/blob/master/index.js#L27

- Linux / centOS
- v6.17.1
- 3.10.10
- N/A
- Own sample script

Wrap up

> Select Y or N for the following statements:

- I contacted the maintainer to let them know: [Y/N] N
- I opened an issue in the related repository: [Y/N] N

Thanks!

Impact

Hello @umarbaloch,

Thank you for your submission! We were able to validate your report, and have submitted it to the appropriate remediation team for review. They will let us know the final ruling on this report, and when/if a fix will be implemented. Please note that the status and severity are subject to change.

Regards,
@lugtag

marcinhoppe Node.js third-party modules staff closed the report and changed the status to ● **Resolved**. Feb 24th (3 years ago)

marcinhoppe Node.js third-party modules staff requested to disclose this report. Feb 24th (3 years ago)

gabriel-kimiaie agreed to disclose this report. Feb 24th (3 years ago)

This report has been disclosed. Feb 24th (3 years ago)