snyk Vulnerability DB

Arbitrary Command Injection

Affecting @acrontum/filesystem-template package,
versions **<0.0.2**

9.8
CRITICAL

Snyk CVSS

INTRODUCED: **6 MAR 2022**   CVE-2022-21186 ❓
CWE-77 ❓   FIRST ADDED BY SNYK

Share ⌄

Exploit Maturity	**Proof of concept** ❓
Attack Complexity	**Low** ❓
Confidentiality	HIGH ❓
Integrity	HIGH ❓
Availability	HIGH ❓

How to fix?

Upgrade @acrontum/filesystem-template to version 0.0.2 or higher.

See more

> NVD   9.8 CRITICAL

Overview

@acrontum/filesystem-template is a Filesystem templating engine and project scaffolding tool

Affected versions of this package are vulnerable to Arbitrary Command Injection due to the `fetchRepo` API missing sanitization of the `href` field of external input.
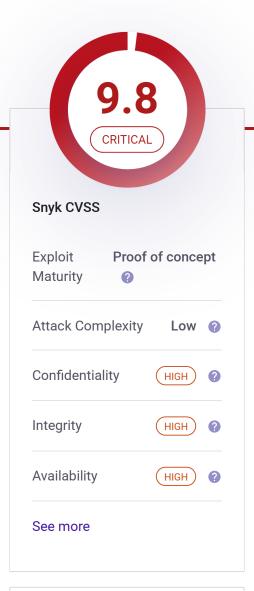
PoC:

```
const filesys = require("@acrontum/filesystem-
template") filesys.fetchRepo({"pathname":"/api/1",
"href": "|touch /tmp/rce", "search":"456" })
```

References

- GitHub Commit

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

Search by package nam

Test your applications

Snyk ID	SNYK-JS-ACRONTUMFILESYSTEMTEMF 2419071
Published	20 Jul 2022
Disclosed	6 Mar 2022
Credit	Feng Xiao, Zhongfu Su

Report a new vulnerability

Found a mistake?

COMPANY

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