

Arbitrary Command Injection

Affecting onion-oled-js package, versions *

INTRODUCED: 23 FEB 2021 CVE-2021-23377 CWE-77 FIRST ADDED BY SNYK Share

How to fix?

There is no fixed version for onion-oled-js .

Overview

onion-oled-js is a JS library that exposes a collection of functions that wrap the oled-exp executable that controls the onion omega OLED display. Affected versions of this package are vulnerable to Arbitrary Command Injection. If attacker-controlled user input is given to the scroll function, it is possible for an attacker to execute arbitrary commands. This is due to use of the child_process exec function without input sanitization.

PoC (provided by reporter):

```
var OLEDExp = require('onion-oled-js').OLEDExp; OLEDExp.scroll(';touch success #');
```

(A file called success will be created as a result of the execution of touch success.)

References

- Vulnerable Code

PRODUCT

- Snyk Open Source
- Snyk Code
- Snyk Container
- Snyk Infrastructure as Code
- Test with Github
- Test with CLI

RESOURCES

- Vulnerability DB
- Documentation
- Disclosed Vulnerabilities
- Blog
- FAQs

COMPANY

CRITICAL

Search by package name or CVE

Snyk CVSS

Exploit Maturity	Proof of concept
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.

Test your applications

Snyk ID	SNYK-JS-ONIONOLEDJS-1078808
Published	18 Apr 2021
Disclosed	23 Feb 2021
Credit	OmniTaint

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



© 2022 Snyk Limited

Registered in England and Wales. Company number: 09677925

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