

Command Injection

Affecting xopen package, versions *

INTRODUCED: 26 JAN 2021 CVE-2020-28447 CWE-78 FIRST ADDED BY SNYK Share

How to fix?

There is no fixed version for xopen .

Overview

xopen is a package that provides a dead-simple Promise API for opening files from Node on Windows, macOS, and Linux. Affected versions of this package are vulnerable to Command Injection. The injection point is located in line 14 in index.js in the exported function xopen(filepath) ##PoC: var root = require("xopen"); var attack_code = "& touch JHU"; root(attack_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-XOPEN-1050981
Published	26 Jan 2021
Disclosed	26 Jan 2021
Credit	JHU System Security Lab

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.