



Look up package or ID...

[About](#) [Advisories](#) [Report Vulnerabilities](#)



## RUSTSEC-2021-0017

[History](#) · [Edit](#)

**Read** on uninitialized buffer may cause UB ( `impl Value for Vec<u8>` )

**Reported** January 30, 2021

**Issued** January 31, 2021 (last modified: October 19, 2021)

**Package** [postscript](#) ([crates.io](#) )

**Type** Vulnerability

**Categories** [memory-exposure](#)

**Aliases** [CVE-2021-26953](#)

**Details** <https://github.com/bodoni/postscript/issues/1>

**CVSS Score** 7.5 HIGH

### CVSS Details

|                            |           |
|----------------------------|-----------|
| <b>Attack vector</b>       | Network   |
| <b>Attack complexity</b>   | Low       |
| <b>Privileges required</b> | None      |
| <b>User interaction</b>    | None      |
| <b>Scope</b>               | Unchanged |
| <b>Confidentiality</b>     | High      |
| <b>Integrity</b>           | None      |
| <b>Availability</b>        | None      |

**CVSS Vector** [CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N](#)

**Patched** `>=0.14.0`

### Description

Affected versions of this crate passes an uninitialized buffer to a user-provided `Read` implementation.

Arbitrary `Read` implementations can read from the uninitialized buffer (memory exposure) and also can return incorrect number of bytes written to the buffer. Reading from uninitialized memory produces undefined values that can quickly invoke undefined behavior.

This flaw was fixed in commit 8026286 by zero-initializing the buffer before handing to a user-provided `Read`.