Reflected Cross Site Scripting affecting SolarWinds: DPA 2021.3.7388 (CVE-2021-35228)

Security Advisory Summary

The vulnerability occurred due to missing input sanitization for one of the output fields extracted from headers on a specific section of a page. An attacker would need to perform a “Man in the Middle” attack to change a header for a remote victim. causing a reflective cross site scripting attack affecting SolarWinds DPA v2021.3.7388.

Affected Products

- DPA 2021.3.7388

Fixed Software Release

- DPA 2021.3.7438

Acknowledgments

- Faris Roslin

Advisory Details

Severity
5.5 Medium

Advisory ID
CVE-2021-35228

First Published
10/19/2021

Fixed Version
DPA 2021.3.7438

CVSS Score
CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:L/A:L