



# CVE-2022-38108

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

|                        |                                                                                                                            |
|------------------------|----------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2022-38108                                                                                                             |
| <b>State</b>           | PUBLIC                                                                                                                     |
| <b>Assigner</b>        | psirt@solarwinds.com                                                                                                       |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                               |
| <b>Published</b>       | 2022-10-20 21:15:00 UTC                                                                                                    |
| <b>Updated</b>         | 2023-03-28 17:15:00 UTC                                                                                                    |
| <b>Description</b>     | SolarWinds Platform was susceptible to the Deserialization of Untrusted Data. This vulnerability allows a remote adversary |

## Risk And Classification

### Problem Types: CWE-502

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor                     | Product                        | Version  | Update  | Edition | Language |
|-------------|----------------------------|--------------------------------|----------|---------|---------|----------|
| Application | <a href="#">Solarwinds</a> | <a href="#">Orion Platform</a> | All      | All     | All     | All      |
| Application | <a href="#">Solarwinds</a> | <a href="#">Orion Platform</a> | 2020.2.6 | -       | All     | All      |
| Application | <a href="#">Solarwinds</a> | <a href="#">Orion Platform</a> | 2020.2.6 | hotfix1 | All     | All      |
| Application | <a href="#">Solarwinds</a> | <a href="#">Orion Platform</a> | 2020.2.6 | hotfix2 | All     | All      |
| Application | <a href="#">Solarwinds</a> | <a href="#">Orion Platform</a> | 2020.2.6 | hotfix3 | All     | All      |
| Application | <a href="#">Solarwinds</a> | <a href="#">Orion Platform</a> | 2020.2.6 | hotfix4 | All     | All      |
| Application | <a href="#">Solarwinds</a> | <a href="#">Orion Platform</a> | 2020.2.6 | hotfix5 | All     | All      |
| Application | <a href="#">Solarwinds</a> | <a href="#">Orion Platform</a> | 2022.2   | All     | All     | All      |
| Application | <a href="#">Solarwinds</a> | <a href="#">Orion Platform</a> | 2022.3   | All     | All     | All      |

## References

| Reference                                                                     | Source  | Link                                                                      | Tags       |
|-------------------------------------------------------------------------------|---------|---------------------------------------------------------------------------|------------|
| SolarWinds Information Service (SWIS) Remote Command Execution ≈ Packet Storm | MISC    | <a href="https://packetstormsecurity.com">packetstormsecurity.com</a>     |            |
| SolarWinds Trust Center Security Advisories   CVE-2022-38108                  | MISC    | <a href="https://www.solarwinds.com">www.solarwinds.com</a>               |            |
| Published   Zero Day Initiative                                               | MISC    | <a href="https://www.zerodayinitiative.com">www.zerodayinitiative.com</a> |            |
| CVE Program record                                                            | CVE.ORG | <a href="https://www.cve.org">www.cve.org</a>                             | canonical  |
| NVD vulnerability detail                                                      | NVD     | <a href="https://nvd.nist.gov">nvd.nist.gov</a>                           | canonical, |

| Vendor Comments And Credit                                                                                                                                                        |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Discovery Credit<br><b>LEGACY:</b> SolarWinds would like to thank Piotr Bazydlo (@chudypb) of Trend Micro Zero Day Initiative for reporting on the issue in a responsible manner. |
| Legacy QID Mappings                                                                                                                                                               |
| <a href="#">377862</a> SolarWinds Orion Platform Multiple Vulnerabilities                                                                                                         |

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**Free CVE JSON API** [cve.report/api](#)

**CVE.report and Source URL Uptime Status** [status.cve.report](#)