



# CVE-2021-35251

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

## Summary

<b>CVE</b>	CVE-2021-35251
<b>State</b>	PUBLIC
<b>Assigner</b>	psirt@solarwinds.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-03-10 17:42:00 UTC
<b>Updated</b>	2022-03-15 00:30:00 UTC
<b>Description</b>	Sensitive information could be displayed when a detailed technical error message is posted. This information could disclose

## Risk And Classification

**Problem Types:** CWE-209

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Solarwinds	Web Help Desk	All	All	All	All

## References

Reference	Source	Link	Tags
Web Help Desk 12.7.8 Release Notes	MISC	<a href="https://documentation.solarwinds.com">documentation.solarwinds.com</a>	
SolarWinds Trust Center Security Advisories   CVE-2021-35251	MISC	<a href="https://www.solarwinds.com">www.solarwinds.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, analysis

## Vendor Comments And Credit

### Discovery Credit

**LEGACY:** SolarWinds would like to thank for Anthony Meluso reporting this vulnerability.

There are currently no legacy QID mappings associated with this CVE.

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](#).

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