



# CVE-2021-42743

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

## Summary

<b>CVE</b>	CVE-2021-42743
<b>State</b>	PUBLIC
<b>Assigner</b>	prodsec@splunk.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-05-06 17:15:00 UTC
<b>Updated</b>	2022-05-17 17:30:00 UTC
<b>Description</b>	A misconfiguration in the node default path allows for local privilege escalation from a lower privileged user to the Splunk user.

## Risk And Classification

**Problem Types:** CWE-427

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Microsoft	Windows	-	All	All	All
Application	Splunk	Splunk	All	All	All	All

## References

Reference	Source	Link	Tags
SVD-2022-0501   Splunk	MISC	<a href="http://www.splunk.com">www.splunk.com</a>	
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

## Vendor Comments And Credit

### Discovery Credit

**LEGACY:** Ilias Dimopoulos of RedyOps Research Labs

## Legacy QID Mappings

[730521](#) Splunk Enterprise Local Privilege Escalation Vulnerability (SVD-2022-0501)

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](#).

**CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)**