



# CVE-2017-5868

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2017-5868
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2017-05-26 01:29:00 UTC
<b>Updated</b>	2017-06-06 14:10:00 UTC
<b>Description</b>	CRLF injection vulnerability in the web interface in OpenVPN Access Server 2.1.4 allows remote attackers to inject arbitrary

## Risk And Classification

**Problem Types:** CWE-93

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Openvpn</a>	<a href="#">Openvpn Access Server</a>	2.1.4	All	All	All
Application	<a href="#">Openvpn</a>	<a href="#">Openvpn Access Server</a>	2.1.4	All	All	All

## References

### Reference

- OpenVPN Access Server Input Validation Flaw Lets Remote Users Conduct Session Fixation Attacks to Hijack a Target User's Session - Secoss-security - [CVE-2017-5868] OpenVPN Access Server : CRLF injection with Session fixation
- [CVE-2017-5868] OpenVPN Access Server : CRLF injection with Session fixation - Sysdream
- CVE Program record
- NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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](#)**