CVE-2017-5868

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2017-5868
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-05-26 01:29:00 UTC
Updated	2017-06-06 14:10:00 UTC
Description	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	Openvpn	Openvpn Access Server	2.1.4	All	All	All
Application	Openvpn	Openvpn Access Server	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 - Secu
oss-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.

CVE.report and Source URL Uptime Status status.cve.report