



# CVE-2015-5965

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

## Summary

|                        |                                                                                                                          |
|------------------------|--------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2015-5965                                                                                                            |
| <b>State</b>           | PUBLIC                                                                                                                   |
| <b>Assigner</b>        | cve@mitre.org                                                                                                            |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                             |
| <b>Published</b>       | 2015-08-11 14:59:00 UTC                                                                                                  |
| <b>Updated</b>         | 2016-12-24 02:59:00 UTC                                                                                                  |
| <b>Description</b>     | The SSL-VPN feature in Fortinet FortiOS before 4.3.13 only checks the first byte of the TLS MAC in finished messages, wh |

## Risk And Classification

### Problem Types: CWE-20

## NVD Known Affected Configurations (CPE 2.3)

| Type             | Vendor   | Product | Version | Update | Edition | Language |
|------------------|----------|---------|---------|--------|---------|----------|
| Operating System | Fortinet | Fortios | All     | All    | All     | All      |

## References

| Reference                                                                                                               | Source   |
|-------------------------------------------------------------------------------------------------------------------------|----------|
| Gentoo Security                                                                                                         | GENTOO   |
| Fortinet FortiGate/FortiOS MAC Authentication Flaw Lets Remote Users Modify Data on the Target System - SecurityTracker | SECTrack |
| FortiGuard                                                                                                              | CONFIRM  |
| Fortinet FortiOS SSL-VPN Man in The Middle Security Bypass Vulnerability                                                | BID      |
| Vivaldi Web Browser Community - 404 - Not Found                                                                         | MISC     |
| CVE Program record                                                                                                      | CVE.ORG  |
| NVD vulnerability detail                                                                                                | NVD      |

No vendor comments have been submitted for this CVE.

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

© [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](#)