



# CVE-2018-16868

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

## Summary

<b>CVE</b>	CVE-2018-16868
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2018-12-03 14:29:00 UTC
<b>Updated</b>	2022-11-30 21:20:00 UTC
<b>Description</b>	A Bleichenbacher type side-channel based padding oracle attack was found in the way gnutls handles verification of RSA d

## Risk And Classification

**Problem Types:** CWE-203

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gnu	Gnutls	All	All	All	All

## References

### Reference

[security-announce] openSUSE-SU-2019:1353-1: important: Security update

1654929 – (CVE-2018-16868) CVE-2018-16868 gnutls: Bleichenbacher-like side channel leakage in PKCS#1 v1.5 verification and padding or

Your browser does not support frames. We recommend upgrading your browser.

[security-announce] openSUSE-SU-2019:1477-1: important: Security update

GNU GnuTLS CVE-2018-16868 Information Disclosure Vulnerability

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](#) 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](#)