



# CVE-2017-1000385

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

## Summary

<b>CVE</b>	CVE-2017-1000385
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2017-12-12 21:29:00 UTC
<b>Updated</b>	2019-10-03 00:03:00 UTC
<b>Description</b>	The Erlang otp TLS server answers with different TLS alerts to different error types in the RSA PKCS #1 1.5 padding. This

## Risk And Classification

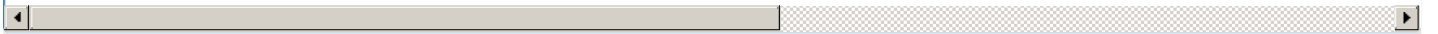
**Problem Types:** CWE-203

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Erlang	Erlang/otp	18.3.4.7	All	All	All
Application	Erlang	Erlang/otp	19.3.6.4	All	All	All
Application	Erlang	Erlang/otp	20.1.7	All	All	All
Application	Erlang	Erlang/otp	18.3.4.7	All	All	All
Application	Erlang	Erlang/otp	19.3.6.4	All	All	All
Application	Erlang	Erlang/otp	20.1.7	All	All	All
Application	Erlang	Erlang/otp	18.3.4.7	All	All	All
Application	Erlang	Erlang/otp	19.3.6.4	All	All	All
Application	Erlang	Erlang/otp	20.1.7	All	All	All

## References

Reference	Source
Red Hat Customer Portal	RE

[SECURITY] [DLA 1207-1] erlang security update	ML
Debian -- Security Information -- DSA-4057-1 erlang	DE
Red Hat Customer Portal	RE
[erlang-questions] Patch Package: OTP 19.3.6.4	ML
The ROBOT Attack - Return of Bleichenbacher's Oracle Threat	MI
USN-3571-1: Erlang vulnerabilities   Ubuntu security notices	UB
Erlang/OTP CVE-2017-1000385 Information Disclosure Vulnerability	BI
[erlang-questions] Patch Package: OTP 18.3.4.7	ML
[erlang-questions] Patch Package: OTP 20.1.7	ML
VU#144389 - TLS implementations may disclose side channel information via discrepancies between valid and invalid PKCS#1 padding	CE
Red Hat Customer Portal	RE
Red Hat Customer Portal	RE
CVE Program record	CV
NVD vulnerability detail	NV
	
<p>No vendor comments have been submitted for this CVE.</p>	
<p>Legacy QID Mappings</p>	
<p><a href="#">296091</a> Oracle Solaris 11.4 Support Repository Update (SRU) 6.1.4 Missing (CPUJAN2019)</p>	

© [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](#).

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