CVE-2017-1000385

MITRE | NVD | CVE.ORG | Print: PDF

Summary

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

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	So
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

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

296091 Oracle Solaris 11.4 Support Repository Update (SRU) 6.1.4 Missing (CPUJAN2019)