CVE-2015-2774

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2015-2774
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-04-07 21:59:00 UTC
Updated	2023-02-21 19:09:00 UTC
Description	Erlang/OTP before 18.0-rc1 does not properly check CBC padding bytes when terminating connections, which makes it eas

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Erlang	Erlang/otp	All	All	All	All
Application	Erlang	Otp	All	All	All	All
Operating System	Opensuse	Opensuse	13.2	All	All	All
Operating System	Opensuse	Opensuse	13.2	All	All	All
Operating System	Oracle	Solaris	11.2	All	All	All
Operating System	Oracle	Solaris	11.2	All	All	All

References

Reference	Source	Link	Tags
Erlang/OTP CVE-2015-2774 Man In The Middle Information Disclosure Vulnerability	BID	www.securityfocus.com	
openSUSE-SU-2016:0523-1: moderate: Security update for erlang	SUSE	lists.opensuse.org	Third Party Adv
oss-security - CVE request: Erlang POODLE TLS vulnerability	MLIST	openwall.com	Third Party Adv
Erlang Programming Language [ANN] Erlang/OTP 18.0-rc1 is available for testing.	CONFIRM	web.archive.org	Release Notes
ImperialViolet - The POODLE bites again	MISC	www.imperialviolet.org	Technical Descr
USN-3571-1: Erlang vulnerabilities | Ubuntu security notices	UBUNTU	usn.ubuntu.com	
oss-security - Re: CVE request: Erlang POODLE TLS vulnerability	MLIST	openwall.com	
Oracle Solaris Third Party Bulletin - April 2015	CONFIRM	www.oracle.com	Third Party Adv

CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analy

No vendor comments have been submitted for this CVE.

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