CVE-2016-7798

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2016-7798
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-01-30 22:59:00 UTC
Updated	2020-11-05 14:56:00 UTC
Description	The openssl gem for Ruby uses the same initialization vector (IV) in GCM Mode (aes-*-gcm) when the IV is set before the k

Risk And Classification

Problem Types: CWE-326

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	Ruby-lang	Openssl	All	All	All	All
Application	Ruby-lang	Openssl	All	All	All	All

References

Reference	Source	Link
oss-security - Re: CVE Request - Ruby OpenSSL Library - IV Reuse in GCM Mode	MLIST	www.openwall.c
cipher: don't set dummy encryption key in Cipher#initialize · ruby/openssl@8108e0a · GitHub	CONFIRM	github.com
[SECURITY] [DLA 1421-1] ruby2.1 security update	MLIST	lists.debian.org
Possible bug: order of setting key vs. IV affects encryption with AES GCM · Issue #49 · ruby/openssl · GitHub	CONFIRM	github.com
Ruby OpenSSL Security Bypass Vulnerability	BID	www.securityfoc
oss-security - CVE Request - Ruby OpenSSL Library - IV Reuse in GCM Mode	MLIST	www.openwall.c
oss-security - Re: CVE Request - Ruby OpenSSL Library - IV Reuse in GCM Mode	MLIST	www.openwall.c
Debian -- Security Information -- DSA-3966-1 ruby2.3	DEBIAN	www.debian.org

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

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

900014 CBL-Mariner Linux Security Update for openssl 1.1.1g

902873 Common Base Linux Mariner (CBL-Mariner) Security Update for Open Secure Sockets Layer (OpenSSL) (2688)