CVE-2012-2130

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2012-2130
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-12-06 18:15:00 UTC
Updated	2019-12-18 20:15:00 UTC
Description	A Security Bypass vulnerability exists in PolarSSL 0.99pre4 through 1.1.1 due to a weak encryption error when generating I

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	8.0	All	All	All
Operating System	Fedoraproject	Fedora	17	All	All	All
Operating System	Fedoraproject	Fedora	17	All	All	All
Application	Polarssl	Polarssl	0.99	pre4	All	All
Application	Polarssl	Polarssl	0.99	pre5	All	All
Application	Polarssl	Polarssl	0.99	pre4	All	All
Application	Polarssl	Polarssl	0.99	pre5	All	All
Application	Polarssl	Polarssl	All	All	All	All

References

Reference	Source	Link
416399 – (CVE-2012-2130) <net-libs/polarssl-1.1.3: Weak key generation (CVE-2012-2130)	MISC	bugs.gentoo.org
PolarSSL Diffie Hellman And RSA Key Exchange Security Bypass Vulnerability	MISC	www.securityfocus.co
CVE-2012-2130	MISC	security-tracker.debia
822639 – (CVE-2012-2130) CVE-2012-2130 polarssl: weak key generation in 0.99pre4 throught to 1.1.1	MISC	bugzilla.redhat.com
IBM X-Force Exchange	MISC	exchange.xforce.ibmc

Gentoo Linux Documentation -- PolarSSL: Multiple vulnerabilities	MISC	security.gentoo.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.

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