



# CVE-2012-2130

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

## Summary

<b>CVE</b>	CVE-2012-2130
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2019-12-06 18:15:00 UTC
<b>Updated</b>	2019-12-18 20:15:00 UTC
<b>Description</b>	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	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	17	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	17	All	All	All
Application	<a href="#">Polarssl</a>	<a href="#">Polarssl</a>	0.99	pre4	All	All
Application	<a href="#">Polarssl</a>	<a href="#">Polarssl</a>	0.99	pre5	All	All
Application	<a href="#">Polarssl</a>	<a href="#">Polarssl</a>	0.99	pre4	All	All
Application	<a href="#">Polarssl</a>	<a href="#">Polarssl</a>	0.99	pre5	All	All
Application	<a href="#">Polarssl</a>	<a href="#">Polarssl</a>	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	<a href="#">bugs.gentoo.org</a>
PolarSSL Diffie Hellman And RSA Key Exchange Security Bypass Vulnerability	MISC	<a href="#">www.securityfocus.co</a>
CVE-2012-2130	MISC	<a href="#">security-tracker.debian</a>
822639 – (CVE-2012-2130) CVE-2012-2130 polarssl: weak key generation in 0.99pre4 through to 1.1.1	MISC	<a href="#">bugzilla.redhat.com</a>
IBM X-Force Exchange	MISC	<a href="#">exchange.xforce.ibmco</a>

Gentoo Linux Documentation -- PolarSSL: Multiple vulnerabilities	MISC	<a href="https://security.gentoo.org">security.gentoo.org</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

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

© [CVE.report](https://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](https://mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://mitre.org/cve). This site includes MITRE data granted under the following [license](https://mitre.org/licenses).

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