



# CVE-2011-0766

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

## Summary

<b>CVE</b>	CVE-2011-0766
<b>State</b>	PUBLIC
<b>Assigner</b>	cert@cert.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2011-05-31 20:55:00 UTC
<b>Updated</b>	2023-09-25 15:28:00 UTC
<b>Description</b>	The random number generator in the Crypto application before 2.0.2.2, and SSH before 2.0.5, as used in the Erlang/OTP s

## Risk And Classification

**Problem Types:** CWE-310

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Erlang</a>	<a href="#">Crypto</a>	1.0	All	All	All
Application	<a href="#">Erlang</a>	<a href="#">Crypto</a>	1.1	All	All	All
Application	<a href="#">Erlang</a>	<a href="#">Crypto</a>	1.1.1	All	All	All
Application	<a href="#">Erlang</a>	<a href="#">Crypto</a>	1.1.2	All	All	All
Application	<a href="#">Erlang</a>	<a href="#">Crypto</a>	1.1.3	All	All	All
Application	<a href="#">Erlang</a>	<a href="#">Crypto</a>	1.2	All	All	All
Application	<a href="#">Erlang</a>	<a href="#">Crypto</a>	1.2.1	All	All	All
Application	<a href="#">Erlang</a>	<a href="#">Crypto</a>	1.2.2	All	All	All
Application	<a href="#">Erlang</a>	<a href="#">Crypto</a>	1.2.3	All	All	All
Application	<a href="#">Erlang</a>	<a href="#">Crypto</a>	1.3	All	All	All
Application	<a href="#">Erlang</a>	<a href="#">Crypto</a>	1.4	All	All	All
Application	<a href="#">Erlang</a>	<a href="#">Crypto</a>	1.5	All	All	All
Application	<a href="#">Erlang</a>	<a href="#">Crypto</a>	1.5.1.1	All	All	All
Application	<a href="#">Erlang</a>	<a href="#">Crypto</a>	1.5.2	All	All	All
Application	<a href="#">Erlang</a>	<a href="#">Crypto</a>	1.5.2.1	All	All	All
Application	<a href="#">Erlang</a>	<a href="#">Crypto</a>	1.5.3	All	All	All
Application	<a href="#">Erlang</a>	<a href="#">Crypto</a>	1.6	All	All	All

Application	<a href="#">Erlang</a>	<a href="#">Crypto</a>	1.6.1	All	All	All
Application	<a href="#">Erlang</a>	<a href="#">Crypto</a>	1.6.2	All	All	All
Application	<a href="#">Erlang</a>	<a href="#">Crypto</a>	1.6.3	All	All	All
Application	<a href="#">Erlang</a>	<a href="#">Crypto</a>	1.6.4	All	All	All
Application	<a href="#">Erlang</a>	<a href="#">Crypto</a>	2.0	All	All	All
Application	<a href="#">Erlang</a>	<a href="#">Crypto</a>	2.0.1	All	All	All
Application	<a href="#">Erlang</a>	<a href="#">Crypto</a>	2.0.2	All	All	All
Application	<a href="#">Erlang</a>	<a href="#">Crypto</a>	1.0	All	All	All
Application	<a href="#">Erlang</a>	<a href="#">Crypto</a>	1.1	All	All	All
Application	<a href="#">Erlang</a>	<a href="#">Crypto</a>	1.1.1	All	All	All
Application	<a href="#">Erlang</a>	<a href="#">Crypto</a>	1.1.2	All	All	All
Application	<a href="#">Erlang</a>	<a href="#">Crypto</a>	1.1.3	All	All	All
Application	<a href="#">Erlang</a>	<a href="#">Crypto</a>	1.2	All	All	All
Application	<a href="#">Erlang</a>	<a href="#">Crypto</a>	1.2.1	All	All	All
Application	<a href="#">Erlang</a>	<a href="#">Crypto</a>	1.2.2	All	All	All
Application	<a href="#">Erlang</a>	<a href="#">Crypto</a>	1.2.3	All	All	All
Application	<a href="#">Erlang</a>	<a href="#">Crypto</a>	1.3	All	All	All
Application	<a href="#">Erlang</a>	<a href="#">Crypto</a>	1.4	All	All	All
Application	<a href="#">Erlang</a>	<a href="#">Crypto</a>	1.5	All	All	All
Application	<a href="#">Erlang</a>	<a href="#">Crypto</a>	1.5.1.1	All	All	All
Application	<a href="#">Erlang</a>	<a href="#">Crypto</a>	1.5.2	All	All	All
Application	<a href="#">Erlang</a>	<a href="#">Crypto</a>	1.5.2.1	All	All	All
Application	<a href="#">Erlang</a>	<a href="#">Crypto</a>	1.5.3	All	All	All
Application	<a href="#">Erlang</a>	<a href="#">Crypto</a>	1.6	All	All	All
Application	<a href="#">Erlang</a>	<a href="#">Crypto</a>	1.6.1	All	All	All
Application	<a href="#">Erlang</a>	<a href="#">Crypto</a>	1.6.2	All	All	All
Application	<a href="#">Erlang</a>	<a href="#">Crypto</a>	1.6.3	All	All	All
Application	<a href="#">Erlang</a>	<a href="#">Crypto</a>	1.6.4	All	All	All
Application	<a href="#">Erlang</a>	<a href="#">Crypto</a>	2.0	All	All	All
Application	<a href="#">Erlang</a>	<a href="#">Crypto</a>	2.0.1	All	All	All
Application	<a href="#">Erlang</a>	<a href="#">Crypto</a>	2.0.2	All	All	All
Application	<a href="#">Erlang</a>	<a href="#">Crypto</a>	All	All	All	All
Application	<a href="#">Erlang</a>	<a href="#">Erlang/otp</a>	r11b-5	All	All	All
Application	<a href="#">Erlang</a>	<a href="#">Erlang/otp</a>	r12b-5	All	All	All
Application	<a href="#">Erlang</a>	<a href="#">Erlang/otp</a>	r13b	All	All	All

Application	Erlang	Erlang/otp	r13b02-1	All	All	All
Application	Erlang	Erlang/otp	r13b03	All	All	All
Application	Erlang	Erlang/otp	r13b04	All	All	All
Application	Erlang	Erlang/otp	r14a	All	All	All
Application	Erlang	Erlang/otp	r14b	All	All	All
Application	Erlang	Erlang/otp	r14b01	All	All	All
Application	Erlang	Erlang/otp	All	All	All	All
Application	Erlang	Erlang/otp	r11b-5	All	All	All
Application	Erlang	Erlang/otp	r12b-5	All	All	All
Application	Erlang	Erlang/otp	r13b	All	All	All
Application	Erlang	Erlang/otp	r13b02-1	All	All	All
Application	Erlang	Erlang/otp	r13b03	All	All	All
Application	Erlang	Erlang/otp	r13b04	All	All	All
Application	Erlang	Erlang/otp	r14a	All	All	All
Application	Erlang	Erlang/otp	r14b	All	All	All
Application	Erlang	Erlang/otp	r14b01	All	All	All
Application	Erlang	Erlang/otp	r14b02	All	All	All
Application	Erlang	Erlang/otp	r11b-5	All	All	All
Application	Erlang	Erlang/otp	r12b-5	All	All	All
Application	Erlang	Erlang/otp	r13b	All	All	All
Application	Erlang	Erlang/otp	r13b02-1	All	All	All
Application	Erlang	Erlang/otp	r13b03	All	All	All
Application	Erlang	Erlang/otp	r13b04	All	All	All
Application	Erlang	Erlang/otp	r14a	All	All	All
Application	Erlang	Erlang/otp	r14b	All	All	All
Application	Erlang	Erlang/otp	r14b01	All	All	All
Application	Erlang	Erlang/otp	All	All	All	All
Application	Ssh	Ssh	1.2.0	All	All	All
Application	Ssh	Ssh	1.2.1	All	All	All
Application	Ssh	Ssh	1.2.10	All	All	All
Application	Ssh	Ssh	1.2.11	All	All	All
Application	Ssh	Ssh	1.2.12	All	All	All
Application	Ssh	Ssh	1.2.13	All	All	All
Application	Ssh	Ssh	1.2.14	All	All	All
Application	Ssh	Ssh	1.2.15	All	All	All

Application	Ssh	Ssh	1.2.16	All	All	All
Application	Ssh	Ssh	1.2.17	All	All	All
Application	Ssh	Ssh	1.2.18	All	All	All
Application	Ssh	Ssh	1.2.19	All	All	All
Application	Ssh	Ssh	1.2.2	All	All	All
Application	Ssh	Ssh	1.2.20	All	All	All
Application	Ssh	Ssh	1.2.21	All	All	All
Application	Ssh	Ssh	1.2.22	All	All	All
Application	Ssh	Ssh	1.2.23	All	All	All
Application	Ssh	Ssh	1.2.24	All	All	All
Application	Ssh	Ssh	1.2.25	All	All	All
Application	Ssh	Ssh	1.2.26	All	All	All
Application	Ssh	Ssh	1.2.27	All	All	All
Application	Ssh	Ssh	1.2.28	All	All	All
Application	Ssh	Ssh	1.2.29	All	All	All
Application	Ssh	Ssh	1.2.3	All	All	All
Application	Ssh	Ssh	1.2.30	All	All	All
Application	Ssh	Ssh	1.2.31	All	All	All
Application	Ssh	Ssh	1.2.4	All	All	All
Application	Ssh	Ssh	1.2.5	All	All	All
Application	Ssh	Ssh	1.2.6	All	All	All
Application	Ssh	Ssh	1.2.7	All	All	All
Application	Ssh	Ssh	1.2.8	All	All	All
Application	Ssh	Ssh	1.2.9	All	All	All
Application	Ssh	Ssh	1.2.0	All	All	All
Application	Ssh	Ssh	1.2.1	All	All	All
Application	Ssh	Ssh	1.2.10	All	All	All
Application	Ssh	Ssh	1.2.11	All	All	All
Application	Ssh	Ssh	1.2.12	All	All	All
Application	Ssh	Ssh	1.2.13	All	All	All
Application	Ssh	Ssh	1.2.14	All	All	All
Application	Ssh	Ssh	1.2.15	All	All	All
Application	Ssh	Ssh	1.2.16	All	All	All
Application	Ssh	Ssh	1.2.17	All	All	All
Application	Ssh	Ssh	1.2.18	All	All	All
Application	Ssh	Ssh	1.2.19	All	All	All

Application	Ssh	Ssh	1.2.2	All	All	All
Application	Ssh	Ssh	1.2.20	All	All	All
Application	Ssh	Ssh	1.2.21	All	All	All
Application	Ssh	Ssh	1.2.22	All	All	All
Application	Ssh	Ssh	1.2.23	All	All	All
Application	Ssh	Ssh	1.2.24	All	All	All
Application	Ssh	Ssh	1.2.25	All	All	All
Application	Ssh	Ssh	1.2.26	All	All	All
Application	Ssh	Ssh	1.2.27	All	All	All
Application	Ssh	Ssh	1.2.28	All	All	All
Application	Ssh	Ssh	1.2.29	All	All	All
Application	Ssh	Ssh	1.2.3	All	All	All
Application	Ssh	Ssh	1.2.30	All	All	All
Application	Ssh	Ssh	1.2.31	All	All	All
Application	Ssh	Ssh	1.2.4	All	All	All
Application	Ssh	Ssh	1.2.5	All	All	All
Application	Ssh	Ssh	1.2.6	All	All	All
Application	Ssh	Ssh	1.2.7	All	All	All
Application	Ssh	Ssh	1.2.8	All	All	All
Application	Ssh	Ssh	1.2.9	All	All	All
Application	Ssh	Ssh	All	All	All	All

## References

Reference	Source	Link
Merge branch 'maint-r14' into dev · erlang/otp@f228601 · GitHub	CONFIRM	<a href="https://github.com">github.com</a>
Erlang/OTP SSH Library Random Number Generator Weakness	BID	<a href="http://www.securityfocus.com">www.securityfocus.com</a>
Erlang/OTP SSH Insecure Random Number Generator Security Issue - Secunia.com	SECUNIA	<a href="http://secunia.com">secunia.com</a>
US-CERT Vulnerability Note VU#178990 - Erlang/OTP SSH library uses a weak random number generator	CERT-VN	<a href="http://www.kb.cert.org">www.kb.cert.org</a>
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="http://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](#) 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](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status [status.cve.report](#)**