CVE-2011-0766

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2011-0766
State	PUBLIC
Assigner	cert@cert.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-05-31 20:55:00 UTC
Updated	2023-09-25 15:28:00 UTC
Description	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	Erlang	Crypto	1.0	All	All	All
Application	Erlang	Crypto	1.1	All	All	All
Application	Erlang	Crypto	1.1.1	All	All	All
Application	Erlang	Crypto	1.1.2	All	All	All
Application	Erlang	Crypto	1.1.3	All	All	All
Application	Erlang	Crypto	1.2	All	All	All
Application	Erlang	Crypto	1.2.1	All	All	All
Application	Erlang	Crypto	1.2.2	All	All	All
Application	Erlang	Crypto	1.2.3	All	All	All
Application	Erlang	Crypto	1.3	All	All	All
Application	Erlang	Crypto	1.4	All	All	All
Application	Erlang	Crypto	1.5	All	All	All
Application	Erlang	Crypto	1.5.1.1	All	All	All
Application	Erlang	Crypto	1.5.2	All	All	All
Application	Erlang	Crypto	1.5.2.1	All	All	All
Application	Erlang	Crypto	1.5.3	All	All	All
Application	Erlang	Crypto	1.6	All	All	All

Application	Erlang	Crypto	1.6.1	All	All	All
Application	Erlang	Crypto	1.6.2	All	All	All
Application	Erlang	Crypto	1.6.3	All	All	All
Application	Erlang	Crypto	1.6.4	All	All	All
Application	Erlang	Crypto	2.0	All	All	All
Application	Erlang	Crypto	2.0.1	All	All	All
Application	Erlang	Crypto	2.0.2	All	All	All
Application	Erlang	Crypto	1.0	All	All	All
Application	Erlang	Crypto	1.1	All	All	All
Application	Erlang	Crypto	1.1.1	All	All	All
Application	Erlang	Crypto	1.1.2	All	All	All
Application	Erlang	Crypto	1.1.3	All	All	All
Application	Erlang	Crypto	1.2	All	All	All
Application	Erlang	Crypto	1.2.1	All	All	All
Application	Erlang	Crypto	1.2.2	All	All	All
Application	Erlang	Crypto	1.2.3	All	All	All
Application	Erlang	Crypto	1.3	All	All	All
Application	Erlang	Crypto	1.4	All	All	All
Application	Erlang	Crypto	1.5	All	All	All
Application	Erlang	Crypto	1.5.1.1	All	All	All
Application	Erlang	Crypto	1.5.2	All	All	All
Application	Erlang	Crypto	1.5.2.1	All	All	All
Application	Erlang	Crypto	1.5.3	All	All	All
Application	Erlang	Crypto	1.6	All	All	All
Application	Erlang	Crypto	1.6.1	All	All	All
Application	Erlang	Crypto	1.6.2	All	All	All
Application	Erlang	Crypto	1.6.3	All	All	All
Application	Erlang	Crypto	1.6.4	All	All	All
Application	Erlang	Crypto	2.0	All	All	All
Application	Erlang	Crypto	2.0.1	All	All	All
Application	Erlang	Crypto	2.0.2	All	All	All
Application	Erlang	Crypto	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	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	github.com
Erlang/OTP SSH Library Random Number Generator Weakness	BID	www.securityfocus
Erlang/OTP SSH Insecure Random Number Generator Security Issue - Secunia.com	SECUNIA	secunia.com
US-CERT Vulnerability Note VU#178990 - Erlang/OTP SSH library uses a weak random number generator	CERT-VN	www.kb.cert.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.