



CVE-2006-0898

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

Summary

CVE	CVE-2006-0898
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-02-25 11:02:00 UTC
Updated	2018-10-18 16:29:00 UTC
Description	Crypt::CBC Perl module 2.16 and earlier, when running in RandomIV mode, uses an initialization vector (IV) of 8 bytes, whi

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Lincoln D. Stein	Crypt Cbc	1.00	All	All	All
Application	Lincoln D. Stein	Crypt Cbc	1.10	All	All	All
Application	Lincoln D. Stein	Crypt Cbc	1.20	All	All	All
Application	Lincoln D. Stein	Crypt Cbc	1.21	All	All	All
Application	Lincoln D. Stein	Crypt Cbc	1.22	All	All	All
Application	Lincoln D. Stein	Crypt Cbc	1.24	All	All	All
Application	Lincoln D. Stein	Crypt Cbc	1.25	All	All	All
Application	Lincoln D. Stein	Crypt Cbc	2.00	All	All	All
Application	Lincoln D. Stein	Crypt Cbc	2.01	All	All	All
Application	Lincoln D. Stein	Crypt Cbc	2.02	All	All	All
Application	Lincoln D. Stein	Crypt Cbc	2.03	All	All	All
Application	Lincoln D. Stein	Crypt Cbc	2.04	All	All	All
Application	Lincoln D. Stein	Crypt Cbc	2.05	All	All	All
Application	Lincoln D. Stein	Crypt Cbc	2.07	All	All	All
Application	Lincoln D. Stein	Crypt Cbc	2.08	All	All	All
Application	Lincoln D. Stein	Crypt Cbc	2.09	All	All	All
Application	Lincoln D. Stein	Crypt Cbc	2.10	All	All	All

Application	Lincoln D. Stein	Crypt Cbc	2.11	All	All	All
Application	Lincoln D. Stein	Crypt Cbc	2.12	All	All	All
Application	Lincoln D. Stein	Crypt Cbc	2.13	All	All	All
Application	Lincoln D. Stein	Crypt Cbc	2.14	All	All	All
Application	Lincoln D. Stein	Crypt Cbc	2.15	All	All	All
Application	Lincoln D. Stein	Crypt Cbc	1.00	All	All	All
Application	Lincoln D. Stein	Crypt Cbc	1.10	All	All	All
Application	Lincoln D. Stein	Crypt Cbc	1.20	All	All	All
Application	Lincoln D. Stein	Crypt Cbc	1.21	All	All	All
Application	Lincoln D. Stein	Crypt Cbc	1.22	All	All	All
Application	Lincoln D. Stein	Crypt Cbc	1.24	All	All	All
Application	Lincoln D. Stein	Crypt Cbc	1.25	All	All	All
Application	Lincoln D. Stein	Crypt Cbc	2.00	All	All	All
Application	Lincoln D. Stein	Crypt Cbc	2.01	All	All	All
Application	Lincoln D. Stein	Crypt Cbc	2.02	All	All	All
Application	Lincoln D. Stein	Crypt Cbc	2.03	All	All	All
Application	Lincoln D. Stein	Crypt Cbc	2.04	All	All	All
Application	Lincoln D. Stein	Crypt Cbc	2.05	All	All	All
Application	Lincoln D. Stein	Crypt Cbc	2.07	All	All	All
Application	Lincoln D. Stein	Crypt Cbc	2.08	All	All	All
Application	Lincoln D. Stein	Crypt Cbc	2.09	All	All	All
Application	Lincoln D. Stein	Crypt Cbc	2.10	All	All	All
Application	Lincoln D. Stein	Crypt Cbc	2.11	All	All	All
Application	Lincoln D. Stein	Crypt Cbc	2.12	All	All	All
Application	Lincoln D. Stein	Crypt Cbc	2.13	All	All	All
Application	Lincoln D. Stein	Crypt Cbc	2.14	All	All	All
Application	Lincoln D. Stein	Crypt Cbc	2.15	All	All	All
Application	Lincoln D. Stein	Crypt Cbc	All	All	All	All

References						
Reference					Source	Link
Lincoln D. Stein Crypt::CBC Perl Module Weak Ciphertext Vulnerability					BID	www.sec
IBM X-Force Exchange					XF	exchange
SUSE Updates for Multiple Packages - Advisories - Secunia					SECUNIA	secunia.c
SecurityFocus					BUGTRAQ	www.sec
Lincoln D. Stein Crypt::CBC Perl Module Weak Ciphertext Vulnerability					SECUNIA	"

rhn.redhat.com Red Hat Support	REDHAT	www.redh
Security Announcement	SUSE	www.nov
SecurityReason	SREASON	securityre
Crypt::CBC RandomIV Header IV Handling Security Issue - Advisories - Secunia	SECUNIA	secunia.c
Debian -- Security Information -- DSA-996-1 libcrypt-cbc-perl	DEBIAN	www.deb
Red Hat update for Red Hat Network Satellite Server - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA	secunia.c
access.redhat.com	REDHAT	rhn.redha
Secunia - Advisories - Debian update for libcrypt-cbc-perl	SECUNIA	secunia.c
Gentoo update for crypt-cbc - Advisories - Secunia	SECUNIA	secunia.c
Gentoo Linux Documentation -- Crypt::CBC: Insecure initialization vector	GENTOO	www.gen
CVE Program record	CVE.ORG	www.cve
NVD vulnerability detail	NVD	nvd.nist.g

No vendor comments have been submitted for this CVE.

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