CVE-2011-3599

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2011-3599
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-10-10 10:55:00 UTC
Updated	2011-10-21 02:56:00 UTC
Description	The Crypt::DSA (aka Crypt-DSA) module 1.17 and earlier for Perl, when /dev/random is absent, uses the Data::Random mo

Risk And Classification

Problem Types: CWE-310

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Adam Kennedy	Crypt-dsa	0.01	All	All	All
Application	Adam Kennedy	Crypt-dsa	0.02	All	All	All
Application	Adam Kennedy	Crypt-dsa	0.03	All	All	All
Application	Adam Kennedy	Crypt-dsa	0.10	All	All	All
Application	Adam Kennedy	Crypt-dsa	0.11	All	All	All
Application	Adam Kennedy	Crypt-dsa	0.12	All	All	All
Application	Adam Kennedy	Crypt-dsa	0.13	All	All	All
Application	Adam Kennedy	Crypt-dsa	0.14	All	All	All
Application	Adam Kennedy	Crypt-dsa	0.15_01	All	All	All
Application	Adam Kennedy	Crypt-dsa	1.16	All	All	All
Application	Adam Kennedy	Crypt-dsa	0.01	All	All	All
Application	Adam Kennedy	Crypt-dsa	0.02	All	All	All
Application	Adam Kennedy	Crypt-dsa	0.03	All	All	All
Application	Adam Kennedy	Crypt-dsa	0.10	All	All	All
Application	Adam Kennedy	Crypt-dsa	0.11	All	All	All
Application	Adam Kennedy	Crypt-dsa	0.12	All	All	All
Application	Adam Kennedy	Crypt-dsa	0.13	All	All	All

Application	Adam Kennedy	Crypt-dsa	0.14	All	All	All
Application	Adam Kennedy	Crypt-dsa	0.15_01	All	All	All
Application	Adam Kennedy	Crypt-dsa	1.16	All	All	All
Application	Adam Kennedy	Crypt-dsa	All	All	All	All
Application	Perl	Perl	All	All	All	All
Application	Perl	Perl	All	All	All	All

References

Reference
oss-security - CVE Request -- perl-Crypt-DSA -- Cryptographically insecure method used for random numbers generation on systems without
oss-security - Re: CVE Request -- perl-Crypt-DSA -- Cryptographically insecure method used for random numbers generation on systems with
76025
Perl Crypt-DSA Module Insecure Random Number Generator Security Issue - Secunia.com
Bug #71421 for Crypt-DSA: Systems without /dev/random may leak secret key
Bug 743567 – CVE-2011-3599 perl-Crypt-DSA: Cryptographically insecure method used for random numbers generation on systems without /
Perl Crypt-DSA Module Random Number Values Security Weakness
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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