CVE-2007-3528

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

Summary

CVE	CVE-2007-3528
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-07-03 18:30:00 UTC
Updated	2008-11-15 06:53:00 UTC
Description	The blowfish mode in DAR before 2.3.4 uses weak Blowfish-CBC cryptography by (1) discarding random bits by the blowfis

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Dar	Dar	All	All	All	All

References

Reference	Source	Link	Tag
#425335 - dar: blowfish encryption weakened by frequent IV collisions - Debian Bug report logs	CONFIRM	bugs.debian.org	
DAR - Disk ARchive / Bugs / #97 blowfish encryption weakened by frequent IV collisions	CONFIRM	sourceforge.net	
38189	OSVDB	osvdb.org	
Disk ARchive Flawed Blowfish-CBC Cryptography Implementation Weakness	BID	www.securityfocus.com	
38190	OSVDB	osvdb.org	
Page not found - SourceForge.net	CONFIRM	sourceforge.net	Patc
DAR Blowfish IV Collision Weakness - Secunia.com	SECUNIA	secunia.com	
Page not found - SourceForge.net	CONFIRM	sourceforge.net	
CVE Program record	CVE.ORG	www.cve.org	canc
NVD vulnerability detail	NVD	nvd.nist.gov	canc

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**