



CVE-2012-2743

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

Summary

CVE	CVE-2012-2743
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-06-27 22:55:00 UTC
Updated	2017-08-29 01:31:00 UTC
Description	Revelation 0.4.13-2 and earlier does not iterate through SHA hashing algorithms for AES encryption, which makes it easier

Risk And Classification

Problem Types: CWE-255

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mikel Olasagasti	Revelation	0.1.0	All	All	All
Application	Mikel Olasagasti	Revelation	0.1.1	All	All	All
Application	Mikel Olasagasti	Revelation	0.1.2	All	All	All
Application	Mikel Olasagasti	Revelation	0.2.0	All	All	All
Application	Mikel Olasagasti	Revelation	0.2.1	All	All	All
Application	Mikel Olasagasti	Revelation	0.3.0	All	All	All
Application	Mikel Olasagasti	Revelation	0.3.1	All	All	All
Application	Mikel Olasagasti	Revelation	0.3.2	All	All	All
Application	Mikel Olasagasti	Revelation	0.3.3	All	All	All
Application	Mikel Olasagasti	Revelation	0.3.4	All	All	All
Application	Mikel Olasagasti	Revelation	0.4.0	All	All	All
Application	Mikel Olasagasti	Revelation	0.4.1	All	All	All
Application	Mikel Olasagasti	Revelation	0.4.10	All	All	All
Application	Mikel Olasagasti	Revelation	0.4.11	All	All	All
Application	Mikel Olasagasti	Revelation	0.4.12	All	All	All
Application	Mikel Olasagasti	Revelation	0.4.2	All	All	All
Application	Mikel Olasagasti	Revelation	0.4.3	All	All	All

4215/1 – (CVE-2012-3818) <x11-misc/revelation-0.4.14 : 100 weak encryption / file format to be considered as a password manager (CVE-2012-3818) - oss-security - CVE Request -- Revelation: 1) Limits effective password length to 32 characters 2) Doesn't iterate the passphrase through SHA-1
oss-security - Re: CVE Request -- Revelation: 1) Limits effective password length to 32 characters 2) Doesn't iterate the passphrase through SHA-1
erikg / Revelation / issues / #61 - File Format Magic String / Version mismatch between Docs and Source — Bitbucket
Revelation Multiple Security Weaknesses
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.