CVE-2012-2146

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

Summary

CVE	CVE-2012-2146
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-08-26 21:55:01 UTC
Updated	2026-04-29 01:13:23 UTC
Description	Elixir 0.8.0 uses Blowfish in CFB mode without constructing a unique initialization vector (IV), which makes it easier for cont

Risk And Classification

Primary CVSS: v2.0 4.3 from nvd@nist.gov

AV:N/AC:M/Au:N/C:P/I:N/A:N

Problem Types: CWE-310 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Partial

Integrity

None

Availability

None

AV:N/AC:M/Au:N/C:P/I:N/A:N

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ematia	Elixir	0.8.0	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source
oss-security - Re: weak use of crypto in python-elixir can lead to information disclosure (CVE and peer review request)	af854a3a-2127-422b
Google Groups	af854a3a-2127-422b
oss-security - Re: weak use of crypto in python-elixir can lead to information disclosure (CVE and peer review request)	af854a3a-2127-422b
810013 – (CVE-2012-2146) CVE-2012-2146 python-elixir: weak use of crypto can leak information	af854a3a-2127-422b
oss-security - weak use of crypto in python-elixir can lead to information disclosure (CVE and peer review request)	af854a3a-2127-422b
#119 ([patch] Encryption scheme doesn't use proper random seed to encrypt) – Elixir – Trac	af854a3a-2127-422b
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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