CVE-2015-0914

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

Summary

CVE	CVE-2015-0914
State	PUBLISHED
Assigner	jpcert
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-05-01 10:59:04 UTC
Updated	2026-05-06 22:30:45 UTC
Description	EasyCTF before 1.4 does not validate the session ID, which allows remote attackers to obtain access via a crafted HTTP re

Risk And Classification

Primary CVSS: v2.0 5 from nvd@nist.gov

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

Problem Types: CWE-284 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

None

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Kozos	Easyctf	All	All	All	All

Vendor Declared Affected Products

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

References

Reference	Source	Link	Tags
Japan Vulnerability Notes/Information from Hiroaki Sakai	af854a3a-2127-422b-91ae-364da2661108	jvn.jp	
JVN#96439865: EasyCTF vulnerable to session management	af854a3a-2127-422b-91ae-364da2661108	jvn.jp	Vendor Advisory
jvndb.jvn.jp/jvndb/JVNDB-2015-000062	af854a3a-2127-422b-91ae-364da2661108	jvndb.jvn.jp	Vendor Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analy

No vendor comments have been submitted for this CVE.

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