



CVE-2010-1872

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

Summary

CVE	CVE-2010-1872
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2010-05-12 11:46:12 UTC
Updated	2026-04-29 01:13:23 UTC
Description	Cross-site scripting (XSS) vulnerability in cPlayer.php in FlashCard 2.6.5 and 3.0.1 allows remote attackers to inject arbitrary

Risk And Classification

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

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

Problem Types: CWE-79 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

None

Integrity

Partial

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Tufat	Flashcard	2.6.5	All	All	All

Application	Tufat	Flashcard	3.0.1	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		
i-MSCP internet - Multi Server Control Panel - Server Default Page		af854a3a-2127-422b-91ae-364da2661108		www.xenuser.org		
FlashCard 'id' Parameter Cross Site Scripting Vulnerability		af854a3a-2127-422b-91ae-364da2661108		www.securityfocus.com		
Files ≈ Packet Storm		af854a3a-2127-422b-91ae-364da2661108		packetstormsecurity.com		
FlashCard "id" Cross-Site Scripting Vulnerability - Advisories - Community		af854a3a-2127-422b-91ae-364da2661108		secunia.com		
CVE Program record		CVE.ORG		www.cve.org		
NVD vulnerability detail		NVD		nvd.nist.gov		
No vendor comments have been submitted for this CVE.						
There are currently no legacy QID mappings associated with this CVE.						