CVE-2011-3642

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

Summary

CVE	CVE-2011-3642
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-02-08 16:15:00 UTC
Updated	2020-02-12 16:54:00 UTC
Description	Cross-site scripting (XSS) vulnerability in Flowplayer Flash 3.2.7 through 3.2.16, as used in the News system (news) extens

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Flowplayer	Flowplayer Flash	All	All	All	All
Application	Flowplayer	Flowplayer Flash	All	All	All	All

References

Reference	So
Bug #1103748 “included flowplayer 3.2.7 is vulnerable” : Bugs : Mahara	MI
Flowplayer 'linkUrl' Parameter Cross Site Scripting Vulnerability	MI
Security Announcements - External vulnerability in Mahara flowplayer in <1.5.8 and <1.6.3 - Mahara ePortfolio System	MI
appsec.ws/Presentations/FlashFlooding.pdf	MI
Security Advisory SA52074 - Mahara Flowplayer Cross-Site Scripting Vulnerability - Secunia	MI
Issue 441 - flowplayer-core - Arbitrary plugins with remote code execution (XSS) - Flowplayer core - Google Project Hosting	MI
Security Advisory SA58854 - TYPO3 News System Extension Flowplayer and Flashmedia Cross-Site Scripting Vulnerabilities - Secunia	MI
Flash Exploitation Database	MI
Security Advisory SA54206 - Flowplayer Flash "plugin" Domain Bypass Cross-Site Scripting Vulnerability - Secunia	MI
Cross-Site Scripting in news - - TYPO3 - The Enterprise Open Source CMS	MI
CVE Program record	CV
NVD vulnerability detail	NV

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**