



CVE-2012-2371

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

Summary

CVE	CVE-2012-2371
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-08-13 20:55:04 UTC
Updated	2026-04-29 01:13:23 UTC
Description	Cross-site scripting (XSS) vulnerability in index.php in the WP-FaceThumb plugin 0.1 for WordPress allows remote attacker

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	Mnt-tech	Wp-facethumb	0.1	All	All	All

Application	Wordpress	Wordpress	-	All	All	All
Vendor Declared Affected Products						
Source	Vendor	Product	Version	Platforms		
CNA	Na	N/a	affected n/a	Not specified		
References						
Reference				Source		
WordPress WP-FaceThumb Gallery 0.1 Cross Site Scripting ~ Packet Storm				af854a3a-2127-422b-91ae-364da26611		
oss-security - Re: CVE-request: WordPress wp-facethumb plugin reflected XSS vulnerability				af854a3a-2127-422b-91ae-364da26611		
Security Alerts - Secunia				af854a3a-2127-422b-91ae-364da26611		
WordPress WP-FaceThumb 'pagination_wp_facethum' Parameter Cross Site Scripting Vulnerability				af854a3a-2127-422b-91ae-364da26611		
[Plugin: WP-FaceThumb] Reflected XSS-vulnerability CWE-79 WordPress.org				af854a3a-2127-422b-91ae-364da26611		
oss-security - CVE-request: WordPress wp-facethumb plugin reflected XSS vulnerability				af854a3a-2127-422b-91ae-364da26611		
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.						