



CVE-2013-4241

Published on: 01/30/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:28 PM UTC

CVE-2013-4241

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Hms Testimonials](#) from [Hitmyserver](#) contain the following vulnerability:

Multiple cross-site scripting (XSS) vulnerabilities in the HMS Testimonials plugin before 2.0.11 for WordPress allow remote attackers to inject arbitrary web script or HTML via the (1) name, (2) image, (3) url, or (4) testimonial parameter to the Testimonial form (hms-testimonials-addnew page); (5) date_format parameter to the

Settings - Default form (hms-testimonials-settings page); (6) name parameter in a Save action to the Settings - Custom Fields form (hms-testimonials-settings-fields page); or (7) name parameter in a Save action to the Settings - Template form (hms-testimonials-templates-new page).

CVE-2013-4241 has been assigned by [secalert@redhat.com](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **HitMyServer - HMS Testimonials** version **before 2.0.11**

CVSS3 Score: **6.1 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
CHANGED	LOW	LOW	NONE

CVSS2 Score: **4.3 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
Full Disclosure: [RCA-201308-01] HMS Testimonials 2.0.10 WP plugin - Multiple vulnerabilities	Exploit Mailing List Third Party Advisory seclists.org text/html	 MISC seclists.org/fulldisclosure/2013/Aug/96
oss-sec: Re: Re: CVE Request - HMS Testimonials 2.0.10 WP plugin	Mailing List Third Party Advisory seclists.org text/html	 MISC seclists.org/oss-sec/2013/q3/361
oss-sec: CVE Request - HMS Testimonials 2.0.10 WP plugin	Mailing List Third Party Advisory seclists.org text/html	 MISC seclists.org/oss-sec/2013/q3/345
WordPress › HMS Testimonials « WordPress Plugins	Release Notes wordpress.org text/html	 MISC wordpress.org/plugins/hms-testimonials/#developers
Full Disclosure: Update [RCA-201309-01] HMS Testimonials 2.0.10 WP plugin - Multiple vulnerabilities	Exploit Mailing List Third Party Advisory seclists.org text/html	 MISC seclists.org/fulldisclosure/2013/Aug/98

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Hitmyserver	Hms Testimonials	All	All	All	All
Application	Hitmyserver	Hms Testimonials	All	All	All	All
<code>cpe:2.3:a:hitmyserver:hms_testimonials:*:*:*:*:wordpress:*:*</code>						
<code>cpe:2.3:a:hitmyserver:hms_testimonials:*:*:*:*:wordpress:*:*</code>						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)