



CVE-2013-6837

Published on: 12/18/2013 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:37 PM UTC

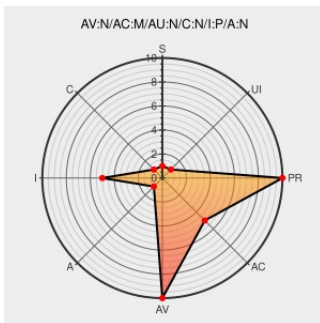
CVE-2013-6837

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Prettyphoto](#) from [No-margin-for-errors](#) contain the following vulnerability:

Cross-site scripting (XSS) vulnerability in the setTimeout function in js/jquery.prettyPhoto.js in prettyPhoto 3.1.4 and earlier allows remote attackers to inject arbitrary web script or HTML via a crafted PATH_INTRO to the default URI.

CVE-2013-6837 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **4.3 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

MEDIUM

Authentication

NONE

Confidentiality
Impact

NONE

Integrity
Impact

PARTIAL

Availability
Impact

NONE

CVE References

Description

Tags

Link

Security Vulnerability
Affecting prettyPhoto
jQuery Script |
ThemeForest
Community Forums

[themeforest.net](#)
[text/html](#)

[MISC themeforest.net/forums/thread/security-vulnerability-affecting-prettyphoto-jquery-script/181180](#)

Haciendo un XSS en
Plugin Prettyphoto ~
Comunidad
PeruCrack

[web.archive.org](#)
[text/html](#)
Inactive Link **Not Archived**

[MISC www.perucrack.net/2014/07/haciendo-un-xss-en-plugin-prettyphoto.html](#)

Update
js/jquery.prettyPhoto.js
· 3ef0ddf ·
Duncaen/prettyphoto ·
GitHub

[Exploit](#)
[Patch](#)
[web.archive.org](#)
[text/html](#)
Inactive Link **Not Archived**

[CONFIRM github.com/Duncaen/prettyphoto/commit/3ef0ddfefebbcc6bbe9245f9cea87e26838e9t](#)

jQuery lightbox for images, videos, YouTube, iframes, ajaxStéphane Caron – No Margin For Errors	www.no-margin-for-errors.com text/html	 CONFIRM www.no-margin-for-errors.com/projects/prettyphoto-jquery-lightbox-clone/
WordPress Pretty Photo Cross Site Scripting - CXSecurity.com	Exploit cxsecurity.com text/html	 MISC cxsecurity.com/issue/WLB-2013110149
WordPress - uDesign - Responsive WordPress Theme ThemeForest	themeforest.net text/html	 CONFIRM themeforest.net/item/udesign-responsive-wordpress-theme/253220
Kali Linux DOM Based XSS Writeup Learn How To Hack - Ethical Hacking and security tips	Exploit www.rafayhackingarticles.net text/html	 MISC www.rafayhackingarticles.net/2013/05/kali-linux-dom-based-xss-writeup.html

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	No-margin-for-errors	Prettyphoto	All	All	All	All
cpe:2.3:a:no-margin-for-errors:prettyphoto:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY 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](#)