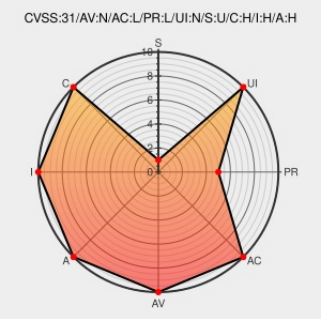
CVE-2015-10087

Published on: Not Yet Published

Last Modified on: 10/20/2023 10:15:00 AM UTC

CVE-2015-10087

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Designfolio-plus from Upthemes contain the following vulnerability:

** UNSUPPPORTED WHEN ASSIGNED ** ** UNSUPPORTED WHEN ASSIGNED ** A vulnerability has been found in UpThemes Theme DesignFolio Plus 1.2 on WordPress and classified as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to unrestricted upload. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of the patch is 53f6ae62878076f99718e5feb589928e83c879a9. It is recommended to apply a patch to fix this issue. The identifier VDB-221809 was assigned to this vulnerability. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.

CVE-2015-10087 has been assigned by cna@vuldb.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **UpThemes** - **Theme DesignFolio Plus** version **= 1.2**

CVSS3 Score: 8.8 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVE References

Description	Tags	Link
WordPress Theme DesignFolio Plus 1.2 upload-file.php Arbitrary File Upload – Alert Logic Support Center	web.archive.org text/html Inactive Link Not Archived	MISC support.alertlogic.com/hc/en-us/articles/360028203692-WordPress-DesignFolio-Plus-1-2-upload-file-php-Arbitrary-File-Upload
Wordpress Theme DesignFolio Plus 1.2 - Arbitrary File Upload	www.exploit-db.com Proof-of-Concept	MISC www.exploit-db.com/exploits/36372

Vulnerability	Proof of Concept text/html	
Login required	vuldb.com text/html Inactive Link Not Archived	MISC vuldb.com/?ctiid.221809
Login required	vuldb.com text/html Inactive Link Not Archived	MISC vuldb.com/?id.221809
WordPress Theme DesignFolio Plus 1.2 - Arbitrary File Upload Vulnerab… · CCrashBandicot/exploit@53f6ae6 · GitHub	github.com text/html	MISC github.com/CCrashBandicot/exploit/commit/53f6ae62878076f99718e5feb589

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	Upthemes	Designfolio-plus	All	All	All	All

cpe:2.3:a:upthemes:designfolio-plus:*:*:*:*:*:wordpress:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→