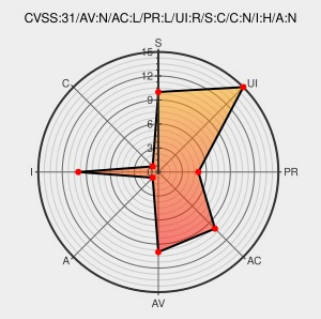
CVE-2020-4047

Published on: 06/12/2020 12:00:00 AM UTC

Last Modified on: 02/27/2023 06:20:00 PM UTC

CVE-2020-4047 - advisory for GHSA-8q2w-5m27-wm27

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



Certain versions of Debian Linux from Debian contain the following vulnerability:

In affected versions of WordPress, authenticated users with upload permissions (like authors) are able to inject JavaScript into some media file attachment pages in a certain way. This can lead to script execution in the context of a higher privileged user when the file is viewed by them. This has been patched in version 5.4.2, along with all the previously affected versions via a minor release (5.3.4, 5.2.7, 5.1.6, 5.0.10, 4.9.15, 4.8.14, 4.7.18, 4.6.19, 4.5.22, 4.4.23, 4.3.24, 4.2.28, 4.1.31, 4.0.31, 3.9.32, 3.8.34, 3.7.34).

CVE-2020-4047 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 6.8 - MEDIUM

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

CVSS2 Score: 3.5 - LOW

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

CVE References

Description	Tags	Link

[SECURITY] Fedora 32 Update: wordpress-5.4.2-1.fc32 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2020-8447a3e195
News – WordPress 5.4.2 Security and Maintenance Release – WordPress.org	Vendor Advisory wordpress.org text/html	MISC wordpress.org/news/2020/06/wordpress-5-4-2-security-and-maintenance-release/
[SECURITY] [DLA 2371-1] wordpress security update	lists.debian.org text/html	MLIST [debian-lts-announce] 20200911 [SECURITY] [DLA 2371-1] wordpress security update
[SECURITY] Fedora 31 Update: wordpress-5.4.2-1.fc31 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2020-bbedd29391
Debian -- Security Information -- DSA-4709-1 wordpress	www.debian.org Depreciated Link text/html	DEBIAN DSA-4709
[SECURITY] [DLA 2269-1] wordpress security update	lists.debian.org text/html	MLIST [debian-lts-announce] 20200701 [SECURITY] [DLA 2269-1] wordpress security update
WordPress: Authenticated XSS via media attachment page · Advisory · WordPress/wordpress-develop · GitHub	Third Party Advisory github.com text/html	CONFIRM github.com/WordPress/wordpress-develop/security/advisories/GHSA-8q2w-5m27-wm27
Editor: Prevent HTML decoding on by setting the proper editor context. · WordPress/wordpress-develop@0977c0d · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/WordPress/wordpress-develop/commit/0977c0d6b241479ecedfe19e96be69f727c3f81f

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All
Operating System	Fedoraproject	Fedora	33	All	All	All
Application	Wordpress	Wordpress	All	All	All	All
Application	Wordpress	Wordpress	All	All	All	All

cpe:2.3:o:debian:debian_linux:10.0:*:*:*:*:*:*:*

cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:*:*

cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:*:*

cpe:2.3:o:fedoraproject:fedora:32:*:*:*:*:*:*:*

cpe:2.3:o:fedoraproject:fedora:33:*:*:*:*:*:*:*

cpe:2.3:a:wordpress:wordpress:*:*:*:*:*:*:*:*

cpe:2.3:a:wordpress:wordpress:*:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)

← Previous ID

Next ID→