EXHIBIT 22

WPScan Vulnerability Disclosure Policy

Last updated: July 26th, 2022.

This policy explains how the WPScan conducts vulnerability disclosures to extension vendors, WPScan users, Jetpack users, security vendors, and the general public in a coordinated and responsible manner.As for better understanding, we will define terms that may be used throughout the policy to avoid ambiguity. They are:

- Coordinator
  - An individual or organization that facilitates the coordinated response process. In this case it's WPScan.
- Reporter
  - The individual or organization that identifies the vulnerability and notifies interested parts (the vendor and/or the coordinator) with the finding.
- Vendor
  - The individual or organization that created or maintains the product that is vulnerable and that must deploy a patch or take other remediation action.
- Marketplace
  - The individual or organization that hosts and distributes the product that is vulnerable, it may be the same individual or organization as the vendor.

Scope

WPScan will evaluate and coordinate the disclosure of any security flaw that can be defined as a weakness in a WordPress application (core or its extensions) and could be exploited or triggered by a threat source.

Initial Contact

WPScan will alert the appropriate Vendor of a security flaw in their affected item(s) in a responsible and timely manner. The initial contact effort will be made using any suitable contacts or formal channels stated on the vendor's website, or by sending an email to security@, support@, info@, and secure@vendor.tld with the relevant details regarding the reported issue.If a Vendor does not respond to WPScan's initial communication within three business days, WPScan may make a second official contact using a different method than the one used earlier, if publicly available.

Deadlines

Vendors are given 30 (thirty) days to resolve the vulnerability with a security patch or other appropriate remedial measure, this is extendable in cases of high complexity, limited to 120 (one hundred and twenty) days after first contact.

Escalation to Marketplace

When the affected item(s) are published in a Marketplace, WPScan will escalate the issue to them if:

- The Vendor fails to reply after an additional two business days following the second notification of the initial contact phase; or
- New versions of the affected item(s) are being released without fixes / attempts to fix the issue; or
- The deadline has been reached and the issue is still not fixed.

Disclosure

policy to avoid ambiguity. They are:

- Coordinator
  - An individual or organization that facilitates the coordinated response process. In this case it's WPScan.
- Reporter
  - The individual or organization that identifies the vulnerability and notifies interested parts (the vendor and/or the coordinator) with the finding.
- Vendor
  - The individual or organization that created or maintains the product that is vulnerable and that must deploy a patch or take other remediation action.
- Marketplace
  - The individual or organization that hosts and distributes the product that is vulnerable, it may be the same individual or organization as the vendor.

Scope

WPScan will evaluate and coordinate the disclosure of any security flaw that can be defined as a weakness in a WordPress application (core or its extensions) and could be exploited or triggered by a threat source.

Initial Contact

WPScan will alert the appropriate Vendor of a security flaw in their affected item(s) in a responsible and timely manner. The initial contact effort will be made using any suitable contacts or formal channels stated on the vendor's website, or by sending an email to security@, support@, info@, and secure@vendor.tld with the relevant details regarding the reported issue.If a Vendor does not respond to WPScan's initial communication within three business days, WPScan may make a second official contact using a different method than the one used earlier, if publicly available.

Deadlines

Vendors are given 30 (thirty) days to resolve the vulnerability with a security patch or other appropriate remedial measure, this is extendable in cases of high complexity, limited to 120 (one hundred and twenty) days after first contact.

Escalation to Marketplace

When the affected item(s) are published in a Marketplace, WPScan will escalate the issue to them if:

- The Vendor fails to reply after an additional two business days following the second notification of the initial contact phase; or
- New versions of the affected item(s) are being released without fixes / attempts to fix the issue; or
- The deadline has been reached and the issue is still not fixed.

Disclosure

WPScan may issue a public alert stating its findings as soon as the Marketplace decides to remove the plugin, or make it unavailable for download on their website.A limited advisory may be issued by WPScan along with a mitigation plan in order to allow the defensive community to safeguard the user if a Vendor is not responsive or unable to make a reasonable argument as to why the vulnerability has not been addressed by the deadline, or if we notice it being actively exploited. We believe that by taking these steps, the vendor will recognize their obligation to their customers and respond appropriately.WPScan will disclose remediated issues with a delay, at its own discretion, to provide affected users feasible time to update their systems. Proof-of-Concept articles will be unpublished for at least one week counting from disclosure date.