WPScan authorised as a Common Vulnerabilities and Exposures Naming Authority by CVE Program

Submitted by: Phiness PR
Tuesday, 12 January 2021

-expertise in protecting WordPress websites recognised by international oversight body-

Bayonne, France, January 12th 2021, WordPress security company, WPScan, has announced that it has been named a Common Vulnerability and Exposures Numbering Authority authorised by the CVE Program to assign CVE IDs to vulnerabilities in Wordpress.

With 75 million users, WordPress is the most popular content management platform in the world and powers 39.6% of all websites, including the New York Times, Forbes, The White House and CNN. WordPress online retail platform, WooCommerce, is used by 27% of the ecommerce market.

Because it is the most popular CMS platform, WordPress also attracts the attention of cyber criminals. To help keep a third of the world's websites protected against hackers, botnet operators and malware distributors, an international army of enthusiasts and cyber security experts constantly check for vulnerabilities that could be exploited. New vulnerabilities are assigned an identification number and added to the Common Vulnerability and Exposures (CVE) List, which is overseen by CVE Numbering Authorities (CNAs).

CNAs are organizations authorised by The CVE Program to assign CVE IDs to vulnerabilities affecting products within their distinct, agreed-upon scope. WPScan has been named a CNA for WordPress core, plugin and theme CVEs.

The CVE Program is the de facto international standard for identifying and naming cyber security vulnerabilities. CVE enables two or more people or tools to refer to a specific vulnerability and know that it is the same one, resulting in significant time and cost savings and aiding mitigation efforts.

WPScan has been actively collecting WordPress core, plugin, and theme vulnerabilities and adding them to its own database since 2014 and has recorded more than 21,875 vulnerabilities in the past seven years. Listed vulnerabilities can be accessed by WPScan users through its API. WPScan also provides its own WordPress security plugin and WordPress security scanner.

Commenting on the company's inclusion in the CVE program, cybersecurity professional and WPScan founder, Ryan Dewhurst said, "WPScan has been diligently researching and collecting WordPress core, plugin and theme vulnerabilities and adding them to its database for seven years. Almost 22,000 vulnerabilities have been identified and added to our database in that time. We are delighted to be recognised as a CVE Numbering Authority, this is a huge accolade for the team and provides additional reassurance to website operators and merchants who rely on WPScan's API, plugins, or scanner to help keep their sites secure."

The CVE Program is driven by a CVE Board, made up of industry, academic and government representatives from around the world. The CVE Program relies on an international community of vendors, end users and researchers who discover and register vulnerabilities. CNAs maintain a community-driven, open data

registry of vulnerabilities, operated on a voluntary basis by participating organisations.

The CVE IDs assigned through the registry enable program stakeholders to rapidly discover and correlate vulnerability information used to protect systems against attacks.

Every CVE Record added to the list is assigned by a CNA and the CVE List feeds the U.S. National Vulnerability Database (NVD).
"I'm excited to have WPScan as an official CVE Numbering Authority," says CVE board member Tod Beardsley. "WPScan has a proven track record of discovering, documenting, and reporting vulnerabilities in popular software that affects a huge population of internet users, and that expertise can only help shape the professionalism of the CVE program."

References:
History of the CVE List: https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=wordpress
The CVE Program: https://cve.mitre.org/
MITRE Corporation: MITRE Corporation: https://www.mitre.org/
MITRE CNA List: https://cve.mitre.org/cve/cna.html
WPScan WordPress PlugIn: https://wordpress.org/plugins/wpscan
WPScan WordPress Scanner https://wpscan.com/wordpress-security-scanner
WPScan on Github: https://github.com/wpscanteam/wpscan

About WPScan:
Founded in 2018, WPScan (https://wpscan.com/) is a service provided by a team of cyber security researchers, led by Ryan Dewhurst, who developed a blackbox scanner which mimics the actions of WordPress hackers. WPScan is available as a CLI scanner, WordPress plugin or API, and offers both free and paid options. WPScan was created for security professionals and WordPress site owners to test the security of their WordPress websites. WPScan’s CLI scanner does not require access to a WordPress dashboard, or source code, therefore, any vulnerabilities it discovers could potentially be exploited by an attacker.
WordPress site owners use WPScan’s scanner, WordPress plugin and API to provide daily scans of their blogs, publications and ecommerce sites, to check that they are using the most up-to-date and secure version of the WordPress software, along with scanning for common vulnerabilities and exposures including weak passwords, which plugins and themes are installed, and whether they have any associated vulnerabilities.
The WPScan WordPress security plugin can be installed from the official WordPress website (https://wordpress.org/plugins/wpscan/).

Media contact:
Josie Herbert
Phiness PR
josie@phinesspr.co.uk
+44 (0)7776 203307