Nexcess Warns Online Retailers To Beware Of Credential Stuffing Attacks

Nexcess, a leading provider of performance-optimized cloud Magento and WooCommerce hosting, has warned eCommerce hosting clients of the risk to stores and customers posed by credential stuffing attacks.

SOUTHFIELD, Mich. (PRWEB) January 31, 2019 -- Nexcess, a leading provider of performance-optimized cloud Magento and WooCommerce hosting, has warned eCommerce hosting clients of the risk to stores and customers posed by credential stuffing attacks. The warning follows the discovery of a massive database of leaked email addresses and passwords.

Credential stuffing relies on the fact that shoppers tend to use the same email and passwords combination on multiple sites. When a password database from one of those sites is leaked and cracked, attackers can use the credentials from that site on other sites. Credential stuffing attacks pose a risk to larger eCommerce stores because there is a strong chance of an attacker finding a username and password combination that grants them access.

The so-called “Collection #1” password dump contains 87 GB of data with over a billion unique passwords and 700 million email addresses. The data comes from 340 compromised passwords databases leaked over many years.

“Online retailers are familiar with the risks posed by brute force and dictionary attacks. Credential stuffing attacks can be just as dangerous,” commented Chris Wells, President and CEO of Nexcess. “At Nexcess, we host thousands of WooCommerce and Magento stores, and we want retailers to be aware of the risk and the steps they can take to mitigate it.”

If shoppers and eCommerce administrators choose long, unique, random passwords, they are protected from all forms of dictionary and credential stuffing attack. Retailers should encourage shoppers to choose adequate passwords and take advantage of the secure password generation features available in browsers, WooCommerce, and many other tools. They may also want to take advantage of the Pwned Password database to warn shoppers of insecure passwords during the account creation process.

Two-factor authentication can also mitigate the impact of credential stuffing attacks. TFA can reduce retail conversion rates, and store owners are often reluctant to implement it for that reason, but providing TFA functionality for administrator logins improves security without impacting shoppers. TFA plugins are available for all major eCommerce applications, including the Nexcess-developed Sentry plugin for Magento.

###

About Nexcess

Nexcess is a Southfield, Michigan-based cloud and managed application hosting company founded in 2000, with data centers distributed throughout the United States, Europe, and Australia. Nexcess offers a variety of performance-optimized and scalable managed cloud hosting solutions for Magento, WordPress, WooCommerce, ExpressionEngine, Craft CMS, and OroCRM. For more information, visit http://www.nexcess.net.
Contact Information
Amy Brueckman
Northcutt
888-908-6272

Online Web 2.0 Version
You can read the online version of this press release here.