# What new security features can we expect to see in the latest version of Magento v1.9.2.4?

rdavis@foregenix.com - 2016-12-22 - Comments (0) - Magento

The latest update to version 1 of Magento includes many general updates and fixes to make the merhcant experience better than ever, while using the popular e-commerece platform.

However, we at Foregenix are more concerned about the security implications and whether previously identified flaws have been corrected. The main technical patch is **SUPEE-7405** which will be discussed today. These patches affect Magento Community Edition prior to v1.9.2.3, and Magento Enterprise Edition prior to v1.14.2.3. Updating to these versions is highly recommended.

The main issues to have been fixed include:

- Stored XSS via email address - APPSEC-1213
    - This fix disallows JavaScript code to be used in an email address when a customer registers with a website. It enabled the administrator session to be stolen an to perform administrative tasks.

- Stored XSS in Order Comments - APPSEC-1239
    - This fix stopped comments with JavaScript, being appending to an order using the *PayFlow Pro* payment module. Magento did not filter the request properly resulting in JavaScript being saved to the database which could then be executed by an administrator who viewe the order. This attack could allow escalation of privalidges and administrator activities.

- Stored XSS in Order - APPSEC-1260
    - In certain configurations, Magento uses the *HTTP_X_FORWARDED_FOR* header as the customer IP address and displays it without sanitization in the Admin Panel. An attacker can use this header to inject JavaScript code into Order View forms in Admin Panel. The code is then executed when a user visits an Order View form, allowing the take over of an administrator session or for an unauthorized user to execute actions on behalf of an administrator. Note that we do not recommend using this header configuration setting.

- Guest order view protection code vulnerable to brute-force attack - APPSEC-1270
    - The guest order view protection code makes it possible to access guest order information for some orders. (This is due to how the code is generated and compared with stored values.) While the attack cannot target a specific order or allow a user to view all orders, it can be used to extract order information from store.

- Malicious files can be upload via backend - APPSEC-1306
    - An administrator can upload a file containing executable code to the server as a logo file if they rename the file to a supported image file format. The issue is not exploitable by itself unless the administrator account that has access to configuration is hacked. However, site audits may flag this issue, and it can cause security audits (such as PCI) to fail.

For help installing patching, go to our other FAQ: here

The fixes here are only a handful of the issues that have been identified and fixed by the Magento development teams. For more information on this update and all other updates, visit Magento's blog: https://magento.com/security/patches/supee-7405

Tags
Magento
Patches
security
SUPEE-7405
v1.9.x.x