New Magento 1.x and 2.x Releases Provide Critical Security and Functional Updates

October 12, 2016

Today, we are releasing several updates that include critical security and functional enhancements.

Enterprise Edition 1.14.3, Community Edition 1.9.3, and SUPEE-8788
Enterprise Edition 1.14.3 and Community Edition 1.9.3 deliver over 120 quality improvements, as well as support for PHP 5.6. **They also resolve critical security issues, including:**

- Remote code execution vulnerabilities with certain payment methods
- Possibility of SQL injections due to Zend Framework library vulnerabilities
- Cross site scripting (XSS) risks with the Enterprise Edition private sale invitation feature
- Improper session invalidation when an Admin user logs out
- The ability for unauthorized users to back up Magento files or databases

The SUPEE-8788 patch addresses these security issues in earlier Magento versions. Functional update details and installation instructions are available in the Enterprise Edition and Community Edition release notes; a full list of security updates is published in the Magento Security Center.

Enterprise Edition and Community Edition 2.0.10 and 2.1.2
Updates to Magento 2 software address the same critical security issues described above. Additionally, the releases make several functional improvements and API enhancements. New API methods allow 3rd party solutions, such as shipping or ERP applications, to use APIs to transition an order state when they create an invoice or shipment. Magento 2.1.2 now also includes PHP 7.0.4 support and Magento 2.0.10 and 2.1.2 are compatible with MySQL 5.7. A summary of improvements is available in the release notes; all security updates are listed in the Security Center.

You are advised to deploy these new releases right away, as attackers may target merchants who are slow to upgrade. Updates should be installed and tested in a development environment before being put into production. Also, please use this occasion to do a security assessment in accordance with our Security Best Practices.

Thank you for your continued cooperation and support.

Best regards,
The Magento Team