National Cyber-Forensics & Training Alliance

NCFTA NOTIFICATION OF PATCHES FOR SHOPLIFT BUG

In early 2015, a well known point-of-sale e-commerce platform, Magento, proactively identified a vulnerability known as Shoplift Bug and subsequently released a patch. The Shoplift Bug continues to pose a threat to e-commerce integrity and financial institutions as merchants patch their point-of-sale systems. Please see below for an updated message from Magento on how to best protect yourself and your customers.

“A recent scan by Byte.nl through the MageReport.com service has indicated that [some sites which use ***Magento Community Edition***] may be vulnerable to the Shoplift security issue. If you have not done so already, we urge you to download and install two previously-released patches that address potential Magento software security risks. The patches should help to prevent an attacker from remotely executing code on Magento software. These issues affect all versions of Magento Community Edition.

RECOMMENDED NEXT STEPS:

- If you are unsure if you have patched your site recently or are a Magento user, please check on MageReport.com to ensure that you have implemented all available security patches correctly.

- Download and implement two patches from the Magento Community Edition download page
    - SUPEE-5344 – Addresses a potential remote code execution exploit (Added Feb 9, 2015)
    - SUPEE-1533 – Addresses two potential remote code execution exploits (Added Oct 3, 2014)

  Note: Different versions of the patch are available for Magento Community Edition 1.4.x through 1.9.x.

- Implement and test the patches in a development environment first to confirm that they work as expected before deploying them to your production site.

- Check for unknown files in the web server document root directory. If you find any, you may be impacted and you should remove unknown files, keeping a secure copy if possible.

- Per Magento security best practices, check all admin accounts to ensure they are all known and authorized. Magento has seen certain admin names used repeatedly such as “system” “testadmin” “service” and various that contain the word “backup”. These are just examples though so you should review each admin account and be assured they can be traced to a specific authorized user. Change all admin passwords if your site has been breached or suspected of a breach.

- Check for unknown IP addresses accessing the system as these may be using legitimate credentials where the password has been guessed but not authorized users. IP addresses that have been reported as examples include 62.76.177.179, 185.22.232.218, [and] 23.245.26.35.

- For community help on installing patches, you can refer to our Community Security patch forum where members of the community, moderators, and Magento can assist with questions about downloading and installing any security patches.

Magento is committed to security as a shared responsibility. To empower merchants' cyber security capacity, we will continue to disseminate/distribute/announce information that can help you identify and resolve potential security issues and defend your network infrastructure. If you wish to ensure that you are notified of these security notifications and alerts, please sign up for the Magento Security Alert Registry."