VISA SECURITY ALERT July 2016

MAGENTO VULNERABILITIES AFFECTING ECOMMERCE MERCHANTS

Distribution: Merchants, Issuers, Acquirers, Processors

Audience: IT, Information Security, Risk Management

Summary

Magento is a popular open-source, e-commerce platform written in PHP. Several critical and high vulnerabilities were discovered and patched on the Magento platform in January 2016. Merchants who have not deployed security patch SUPEE-7405, as required by PCI standards, are vulnerable to remote exploits that can compromise account data.

Description and Impact

In late 2015, security firm Sucuri and other researchers reported a number of vulnerabilities to the Magento bug bounty program, which included cross-site scripting (XSS) as well as a cross-site request forgery (CSRF) vulnerability reported by other security firms. These issues, along with others discovered through internal analysis, were addressed by a security patch, SUPEE-7405, in January 2016. At the time of release, Magento had no reports of attackers exploiting these weaknesses. Other vulnerabilities included insufficient protection, formula injection, denial-of-service (DoS), and brute force issues. Several of these vulnerabilities potentially allow an attacker to take over administrative privileges in the merchant's e-commerce environment.

One XSS flaw potentially allows an attacker to add malicious JavaScript code to a comment via the PayFlow Pro payment module. The JavaScript code is executed server-side when the targeted site's administrator views the attacker's order . The stored cross-site scripting (XSS) bug is present in versions of Magento Community Edition and Enterprise Edition prior to 1.9.2.3 and 1.14.2.3, respectively.

The cross-site request forgery (CSRF) vulnerability allows an attacker to potentially exploit this flaw by tricking an administrator into clicking on a specially crafted link through phishing. In addition to the XSS and CSRF discovered vulnerabilities, another high severity information disclosure bug was found in Magento's RSS feed and it was determined that an attacker could potentially download order-related information by using special parameters in the RSS feed request.

The following Magento versions, when deployed without a proper web application firewall, are vulnerable to the issues described above:

- Community Edition versions prior to 1.9.2.3
- Enterprise Edition versions prior to 1.14.2.3

Detection and Mitigation

For those merchants using Magento in their e-commerce environment, the first step is to determine the Magento edition and version used. It's important that merchant administrators install security patch SUPEE-7405 as quickly as possible to address these issues, and to regularly check for new patches to protect their sites and comply with PCI standards. While the issues covered by this alert were discovered through a bug bounty program, attackers are targeting merchants who have been slow to deploy patches after they are released. Information about all security patches is posted on the Magento Security Center (https://magento.com/security) and merchants can sign up to receive alerts whenever new security patches or advisories are published at https://magento.com/security/sign-up. Magento also attempts to notify customers via email and RSS messages in their Magento Admin regarding new patches.

Magento previously released the SUPEE-5344 security patch in January 2015. It is recommended that all merchants implement the patch as soon as possible to protect against the RCE vulnerability. In addition to installing the recommended security patches, merchants should use a web application firewall to reduce their exposure.

External Links:

- Magento Security Best Practices: https://magento.com/security/best-practices/security-best-practices
- Magento Security Patches: https://magento.com/security/patches/supee-7405
- Common Vulnerabilities & Exposures: CVE-2015-1397, CVE-2015-1398, CVE-2015-1399, CVE-2015-2068

To report a data breach, contact Visa Fraud Control:

- Asia Pacific Region, Central Europe/Middle East/Africa Region: VIFraudControl@visa.com
- U.S. and Canada: USFraudControl@visa.com

For more information, please contact Visa Risk Management: cisp@visa.com