MASTERCARD CYBER AND INTELLIGENCE SOLUTIONS

URGENT REMINDER TO ACQUIRERS THAT MAGENTO 1 WILL NO LONGER BE SUPPORTED BY ADOBE AFTER JUNE 2020

MAGENTO 1 SUNSETTING

June 30, 2020 will mark the end of Adobe's support for Magento 1. Its successor, Magento 2 (released in 2015) is the current supported version of the Magento platform[1]. Merchants still using the Magento 1 platform after June 2020 must take steps to ensure that they remain compliant with the Payment Card Industry Data Security Standard (PCI DSS). Adobe has announced that they will not be providing patches to Magento 1 after June 2020. Merchants that continue to use Magento 1 after June 30, 2020 are at an elevated risk of suffering a data breach and may not be compliant with the PCI DSS. Merchants must upgrade to Magento 2 or take appropriate steps to ensure that the vulnerability cannot be exploited. (Mastercard is aware of several 3rd party companies offering continued support for Magento 1).

In order to remain PCI DSS compliant after June 30, 2020, merchants still using Magento 1 must ensure that vulnerabilities discovered in Magento 1 remain unexploitable. Acquirers should work with their merchants to ensure they are using the latest version of Magento, or another supported platform, in order to remain PCI DSS compliant after June 30, 2020 and to meet Mastercard Site Data Protection (SDP) Program Standards. For more information on merchant PCI compliance validation requirements, Mastercard SDP Standards can be found in the Security Rules and Procedures on Mastercard Connect™.

GROWING DIGITAL SKIMMING CONCERNS

The Mastercard Account Data Compromise (ADC) team is responsible for investigating global events that impact cardholder data. Analysis of current investigations clearly indicate that merchants operating on a platform that is not regularly supported with quality fixes and security patches by the platform vendor become an easy target for criminals looking to exploit known vulnerabilities. In fact, it has been revealed through ADC events that 77% of companies investigated were not in compliance with PCI DSS requirement 6 (develop and maintain secure systems and applications) at time of the breach.

Over the past three years, an increasing number of merchant data breaches have been executed via digital skimming techniques. "Digital skimming," also called "Magecart" or "Form-jacking," describes an attack method that targets e-commerce merchants. Attackers exploit vulnerabilities to insert malicious scripts into the source code of merchant checkout pages to exfiltrate cardholder data and other sensitive information. A common trend observed by investigators and global researchers is that many websites impacted by this attack-style are running older versions of Magento.[2,3] With the additional increase in digital skimming attacks driven by the ongoing COVID-19 pandemic[4], Mastercard reminds Acquirers that merchants still using Magento 1 may be targeted.

RISKRECON TO MONITOR MAGENTO TRENDS

Mastercard recently acquired RiskRecon for the purpose of expanding and enhancing account data compromise and breach detection by integrating cyber risk assessment and remediation for issuers and acquirers. Using non-invasive techniques, RiskRecon helps hundreds of organizations better understand and act on their enterprise cybersecurity health by continuously discovering their digital footprint and assessing their cybersecurity across over 40 security criteria spanning thousands of security checks. Leveraging this technology, Mastercard will work with acquiring banks to ensure they are aware of their merchants using end of life software such as Magento 1.

RESOURCES

- RiskRecon Free Cybersecurity Assessments - https://blog.riskrecon.com/free-cybersecurity-assessments
- Mastercard Site Data Protection Program (SDP) - https://www.mastercard.us/en-us/business/overview/safety-and-security/security-recommendations/site-data-protection-PCI.html
- Mastercard Global Risk - https://globalrisk.mastercard.com/
- Mastercard Account Data Compromise Best Practice Manual - https://globalrisk.mastercard.com/wp-content/uploads/2019/08/ADC-Best-Practice-Manual.pdf
- Magento End of Support Announcement - https://magento.com/blog/magento-news/supporting-magento-1-through-june-2020
- Magento Lifecycle Policy - https://magento.com/sites/default/files/magento-software-lifecycle-policy.pdf

CONTACT EMAILS: ADC@mastercard.com – RiskRecon@mastercard.com – sdp@mastercard.com

---

1 Magento.com. n.d. MAGENTO SOFTWARE LIFECYCLE POLICY. [online] Available at: <https://magento.com/sites/default/files/magento-software-lifecycle-policy.pdf?_ga=2.17189817.1484339484.1591215587-1149984847.1589309707>
2 Seals, T., 2019. Magecart Hits 80 Major Ecommerce Sites in Card-Skimming Bonanza. [online] Threatpost.com. Available at: <https://threatpost.com/magecart-ecommerce-card-skimming-bonanza/147765/>
3 Cimpanu, C., 2020. FBI Issues Warning About E-Skimming (Magecart) Attacks | ZDnet. [online] ZDNet. Available at: <https://www.zdnet.com/article/fbi-issues-warning-about-e-skimming-magecart-attacks/>
4 Newman, L., 2020. Online Credit Card Skimmers Are Thriving During the Pandemic. [online] Wired. Available at: https://www.wired.com/story/magecart-credit-card-skimmers-coronavirus-pandemic/