Acquirer Advisory - Urgent Action Required - Magento 1 support to end after June 2020

April 2020

VISA everywhere you want to be

ABOUT THIS GUIDE:

Useful information to highlight the upcoming end of life for Magento 1 platform

Overview

Visa is committed to enhancing both the security and quality of payment services available in both Card-Present and Card-Not-Present environments. This fact sheet provides useful information related to the upcoming end of life for all Magento 1 websites. Merchants must be cognizant of their responsibilities in securing their environment to help prevent the loss of payment card data. Acquirers should use this information to take risk-based decisions and encourage their merchants to migrate to a supported version or alternate platform to remain PCI compliant.

Merchants who suspect or confirm a compromise involving payments data must adhere to the requirements outlined in Visa's What To Do If Compromised guide.

Designed to highlight the upcoming end date for support of Magento 1.

Content Section

Urgent Action Required - Magento 1 Unsupported after June 2020

When Magento announced the release of Magento 2 in November 2015, merchants and developers alike were made aware that Magento 1 would become obsolete.

The original end date for support of Magento 1 was November 2018, however, this was revised to June 2020 after concerns were raised that the original timeframe did not provide sufficient opportunity for merchants and Magento developers to migrate Magento 1 websites, which includes both Magento Commerce 1 (formerly known as Enterprise Edition) and Magento Open Source 1 (formerly known as Community Edition).

Given the absence of security patches after the revised cut-off date, any sites that have failed to migrate will be vulnerable to security breaches *and* pose an increased risk to the security of payment card data.

Steps for those migrating:

Merchants considering the transition to Magento 2.3 should view this as more than just a simple "version upgrade" or "migration."

Effectively, Magento 2.3 is an entirely new platform with substantial framework differences from Magento 1. To ensure success, the transition effort should be considered as a new build or full rebuild project. Merchants will need to find the Magento 2.3-compatible version of their extensions and custom code will need to be reviewed, rewritten, and made compatible with Magento 2.3. These efforts are often large and involved, thus, merchants should begin the process and start upgrading immediately, referencing Magento's Software Lifecycle Policy

Consequences of not migrating:

Since official support for Magento 1 is ending after June 2020, running the web and software applications after this cut-off date creates a number of risks, such as:

- Without any upgrade or security patches, merchants' ecommerce sites may degrade and become unstable;
- Extensions or plug-ins functionality may break or become unavailable;
- Over time, Magento developers will only be familiar with Magento 2;
- Merchants will fall out of compliance with PCI DSS; and
- Ecommerce sites will be more exposed to security risks and increased likelihood of an account data compromise due to the lack of security upgrades.

Payment Card Industry Data Security Standards (PCI DSS) Compliance:

PCI DSS Requirements 6.1 and 6.2 address the need to keep systems up to date with vendor-supplied security patches to protect systems from known vulnerabilities. Hence, failing to migrate a Magento 1 ecommerce website will cause merchants to fall out of PCI DSS compliance because no security patch will be available for new vulnerabilities after June 2020. Specifically, a merchant is required to have policies and procedures, and be able to demonstrate that its implementation satisfies Requirement 6: Develop and maintain secure systems and applications:

6.1 Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as "high," "medium," or "low") to newly discovered security vulnerabilities.

6.2 Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release.

Further, these merchants may also fail to obtain a passing Approved Scanning Vendor (ASV) scan if they are unable to address the vulnerabilities detected in their Magento 1 websites.

Therefore, it is imperative that impacted merchants migrate before the end of June 2020 to maintain PCI DSS compliance and to ensure that their Acquirer's portfolios are protected.

The latest set of PCI DSS requirements can be found here:

https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf

Proactively working with your merchants to protect their environment can help prevent data loss and fraud across the ecosystem.

Data Compromise Implications – What To Do If Compromised Guide

Visa is dedicated to promoting the safe and sound long-term prosperity of the Visa payment system. To that end, Visa aims to ensure the timely resolution of external data Compromise Events, drive notification of at-risk accounts to stem fraud impacts, and synthesize forensic evidence, intelligence, and fraud analysis to formulate remediation plans that strengthen payment system security.

Merchants running the Magento 1 web and software applications after the cut-off date increase the risk of an account data compromise event.

Any entity that suspects or confirms unauthorized access to any Visa cardholder data, including any entity that stores, processes, or transmits cardholder data or has access to a payments environment or systems is required to adhere to the What To Do If Compromised (WTDIC) requirements.

WTDIC establishes procedures and timelines for reporting and responding to a suspected or confirmed Compromise Event. To mitigate payment system risk during a Compromise Event, prompt action is required to prevent additional exposure, including ensuring containment actions and remediation, such as confirming that proper PCI DSS and PCI PIN Security controls are in place and are functioning correctly.

The What To Do If Compromised Guide can be found here:
https://usa.visa.com/dam/VCOM/download/merchants/cisp-what-to-do-if-compromised.pdf