25 Adobe Vulnerabilities in Commerce and Magento Products

Overview

Adobe has released urgent security patches addressing 25 vulnerabilities in its Commerce and Magento Open-Source platforms. The most severe of these vulnerabilities include code execution, privilege escalation, and security bypass risks, with two vulnerabilities rated as critical with CVSS scores of 9.8 and 8.8. The vulnerabilities are as follows:

CVE-2024-45115 (CVSS 9.8)	**CVE-2024-45125** (CVSS 4.3)
CVE-2024-45148 (CVSS 8.8)	**CVE-2024-45127** (CVSS 4.8)
CVE-2024-45116 (CVSS 8.1)	**CVE-2024-45128** (CVSS 5.4)
CVE-2024-45117 (CVSS 7.6)	**CVE-2024-45129** (CVSS 4.3)
CVE-2024-45118 (CVSS 6.5)	**CVE-2024-45130** (CVSS 4.3)
CVE-2024-45119 (CVSS 5.5)	**CVE-2024-45131** (CVSS 5.4)
CVE-2024-45120 (CVSS 4.3)	**CVE-2024-45132** (CVSS 6.5)
CVE-2024-45121 (CVSS 4.3)	**CVE-2024-45133** (CVSS 2.7)
CVE-2024-45122 (CVSS 4.3)	**CVE-2024-45134** (CVSS 2.7)
CVE-2024-45123 (CVSS 6.1)	**CVE-2024-45135** (CVSS 2.7)
CVE-2024-45124 (CVSS 5.3)	**CVE-2024-45149** (CVSS 2.7)

The vulnerabilities impact Adobe Commerce versions 2.4.7-p2 and earlier, as well as Magento Open Source 2.4.7-p2 and earlier. Although there are no known active exploits for these vulnerabilities at this time, Aspire recommends immediate updates to mitigate.

Aspire Protects

- **Apply Patches** – Users should update Adobe Commerce and Magento Open Source to the latest patched versions:
  - Adobe Commerce: Version 2.4.7-p3 or higher.
  - Magento Open Source: Version 2.4.7-p3 or higher.
  - CVE-2024-45115 - This critical vulnerability requires an isolated patch for Adobe Commerce B2B. Ensure B2B versions between 1.3.3 and 1.4.2 are patched accordingly.
  - Find patch guidance in Adobe's security advisory.

IoCs

There are no known IoCs associated with the above vulnerabilities at this time. Aspire is actively monitoring and will notify customers if any are found. For more details on how we can help protect your organization, contact Aspire's Customer Success Management team.

TTPs to Watch

CVE-2024-45115

- Initial Access (TA0001)
  - Exploit Public-Facing Application (T1190) – Attackers can exploit the improper authentication flaw in public-facing applications to gain initial access to affected systems.
- Privilege Escalation (TA0004)
  - Exploitation for Privilege Escalation (T1068) – Attackers can exploit improper authentication to escalate privileges on affected systems without requiring admin credentials.
- Initial Access (TA0001)
  - Exploit Public-Facing Application (T1190) – Attackers can exploit the improper authentication flaw in public-facing applications to gain initial access to affected systems.

Aspire's Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors. Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyberattacks.
- **Aspire Managed Security Services**
  - Aspire Managed Security Services provide remote security monitoring and device management – 24 hours a day, 7 days a week. By aggregating and correlating security events from across your IT environment, our remote security monitoring service eliminates "noise" and make sense of what really matters.
  - Our managed security portfolio includes:
    - Managed Firewall

- Managed IDS/IPS
- Security event monitoring & incident management
- Managed Cisco ISE (Identity Services Engine)
- Endpoint Protection

Supporting Documentation

Adobe Security Bulletin

Adobe Security Bulletin