Hive Pro

THREAT ADVISORY

Critical Magento zero-day vulnerability actively exploiting multiple e-commerce websites

TA2022031

Threat Level **RED**

Publish Date – Feb 14, 2022
Updated Date – Feb 18, 2022

Adobe issued an emergency advisory informing Adobe Commerce and Magento Open-Source product users of a critical zero-day vulnerability that is being actively exploited in the wild.

A zero-day vulnerability which has been assigned CVE-2022-24086 affects the Adobe Commerce and Magento Open-Source products as they fail to properly validate the user input. A pre-authenticated attacker can exploit this to execute arbitrary code on the victim's machine. This vulnerability is being exploited in the wild and targeting Adobe Commerce merchants.

Only three days later, Adobe updated same security advisory for the new vulnerability which is related to the earlier reported zero-day vulnerability (CVE-2022-24086) and assigned it CVE-2022-24087. This update has been issued for a new vulnerability that fixes the zero-day vulnerability's incomplete patch.

Hive Pro threat research team advices organizations to patch these vulnerabilities as soon as possible using the patch links below.

Potential MITRE ATT&CK TTPs are:
TA0001: Initial Access
TA0002: Execution
TA0003: Persistence
TA0004: Privilege Escalation
TA0005: Defense Evasion
T1190: Exploit Public-Facing Application
T1078: Valid Accounts
T1068: Exploitation for Privilege Escalation

Vulnerability Details

CVE ID	Affected Products	Affected CPE	Vulnerability Name	CWE ID
CVE-2022-24086	Adobe Commerce and Magento Open Source 2.3.3 to-2.3.7-p2 and 2.4.0 to 2.4.3-p1	cpe:2.3:a:magento:magento:*:*:*:*:*:*:*:*	Adobe Commerce and Magento Open-Source code execution	CWE-20
CVE-2022-24087	Adobe Commerce and Magento Open Source 2.3.3 to-2.3.7-p2 and 2.4.0 to 2.4.3-p1	cpe:2.3:a:magento:magento:*:*:*:*:*:*:*:*	Adobe Commerce and Magento Open-Source code execution	CWE-20

Patch Link

https://github.com/magento/knowledge-base/blob/main/src/troubleshooting/known-issues-patches-attached/assets/MDVA-43395_EE_2.4.3-p1_COMPOSER_v1.patch.zip?raw=true
https://github.com/magento/knowledge-base/blob/main/src/troubleshooting/known-issues-patches-attached/assets/MDVA-43443_EE_2.4.3-p1_COMPOSER_v1.patch.zip?raw=true
https://github.com/magento/knowledge-base/blob/main/src/troubleshooting/known-issues-patches-attached/assets/MDVA-43395_EE_2.4.3-p1_v1.patch.zip?raw=true
https://github.com/magento/knowledge-base/blob/main/src/troubleshooting/known-issues-patches-attached/assets/MDVA-43443_EE_2.4.3-p1_v1.patch.zip?raw=true
https://github.com/magento/knowledge-base/blob/main/src/troubleshooting/known-issues-patches-attached/assets/MDVA-43443_EE_2.4.2-p2_COMPOSER_v1.patch.zip?raw=true
https://github.com/magento/knowledge-base/blob/main/src/troubleshooting/known-issues-patches-attached/assets/MDVA-43443_EE_2.4.2-p2_v1.patch.zip?raw=true
https://github.com/magento/knowledge-base/blob/main/src/troubleshooting/known-issues-patches-attached/assets/MDVA-43443_EE_2.3.4_COMPOSER_v1.patch.zip?raw=true
https://github.com/magento/knowledge-base/blob/main/src/troubleshooting/known-issues-patches-attached/assets/MDVA-43443_EE_2.3.4_v1.patch.zip?raw=true

References

https://helpx.adobe.com/security/products/magento/apsb22-12.html
https://support.magento.com/hc/en-us/articles/4426353041293-Security-updates-available-for-Adobe-Commerce-APSB22-12-