

HiveForce Labs

# THREAT ADVISORY

 **VULNERABILITY REPORT**

## Hackers Pocket Payment Data via Magento Exploitation

Date of Publication

April 8, 2024

Admiralty Code

A1

TA Number

TA2024133

# Summary

**First Seen:** February 13, 2024

**Affected Product:** Adobe Commerce, Magento

**Impact:** Cyber attackers have exploited a previously addressed critical vulnerability in Magento, known as CVE-2024-20720. They are specifically targeting e-commerce platforms to distribute a Stripe payment skimmer, crafted for covertly extracting financial data.

## ⚙️ CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2024-20720	Adobe OS Command Injection Vulnerability	Adobe Commerce, Magento	❌	❌	✅

# Vulnerability Details

## #1

Attackers are exploiting a previously addressed critical Magento vulnerability, identified as CVE-2024-20720. This exploitation targets e-commerce platforms, enabling the distribution of a Stripe payment skimmer intended for illicit financial data extraction. The vulnerability in question, CVE-2024-20720, stems from an Adobe flaw, allowing for the improper neutralization of special elements, thereby creating pathways for arbitrary code execution.

## #2

Perpetrators have devised a novel technique for embedding malware persistently within Magento servers. They accomplish this by embedding a meticulously crafted layout template directly into the database, acting as a conduit for automated malware injection. By combining the Magento layout parser with the assert package, which is pre-installed, attackers can execute system commands seamlessly.

# #3

This results in the establishment of a remote code execution backdoor, enabling the deployment of a Stripe payment skimmer to covertly capture and transmit financial data to a site controlled by the attacker. The exploitation of this vulnerability hinges on the attacker being authenticated. The exploit requires administrative privileges, limiting its feasibility to attackers with such elevated access. Furthermore, the exploitation of this vulnerability does not necessitate any user interaction.

## Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-20720	Adobe Commerce: 2.3.7 - 2.4.6-p3, Magento Open Source: 2.4.4 - 2.4.6-p3	cpe:2.3:a:adobe:commerce:-:*:*:*:*:*	CWE-78

## Recommendations



**Apply Official Fixes Immediately:** While upgrading to a patched version of Adobe is crucial, it's advisable to implement additional security measures regardless. This ensures comprehensive protection against potential vulnerabilities.



**Least Privilege Principle:** Follow the principle of least privilege by granting users and processes only the permissions necessary to perform their tasks. This minimizes the potential damage that can be caused by compromised accounts or processes.



**Vendor and Third-Party Risk Management:** Regularly assess the security posture of third-party vendors and service providers involved in the e-commerce ecosystem. Ensure that vendors adhere to security best practices and compliance requirements to minimize supply chain risks.



**Vulnerability Management:** This involves regularly assessing and updating software to address known vulnerabilities. Maintain an inventory of software versions and security patches, and evaluate the security practices of third-party vendors, especially for critical applications and services.

# Potential MITRE ATT&CK TTPs

<b><u>TA0001</u></b> Initial Access	<b><u>TA0002</u></b> Execution	<b><u>TA0007</u></b> Discovery	<b><u>TA0003</u></b> Persistence
<b><u>TA0004</u></b> Privilege Escalation	<b><u>TA0040</u></b> Impact	<b><u>T1588</u></b> Obtain Capabilities	<b><u>T1059</u></b> Command and Scripting Interpreter
<b><u>T1082</u></b> System Information Discovery	<b><u>T1588.002</u></b> Tool	<b><u>T1587.004</u></b> Exploits	<b><u>T1567</u></b> Exfiltration Over Web Service
<b><u>T1083</u></b> File and Directory Discovery	<b><u>T1659</u></b> Content Injection	<b><u>T1546</u></b> Event Triggered Execution	<b><u>T1068</u></b> Exploitation for Privilege Escalation
<b><u>T1055</u></b> Process Injection	<b><u>T1543</u></b> Create or Modify System Process	<b><u>T1657</u></b> Financial Theft	

## Patch Details

Upgrade your Magento to 2.4.6-p4, 2.4.5-p6 or 2.4.4-p7

Link:

<https://helpx.adobe.com/security/products/magento/apsb24-03.html>

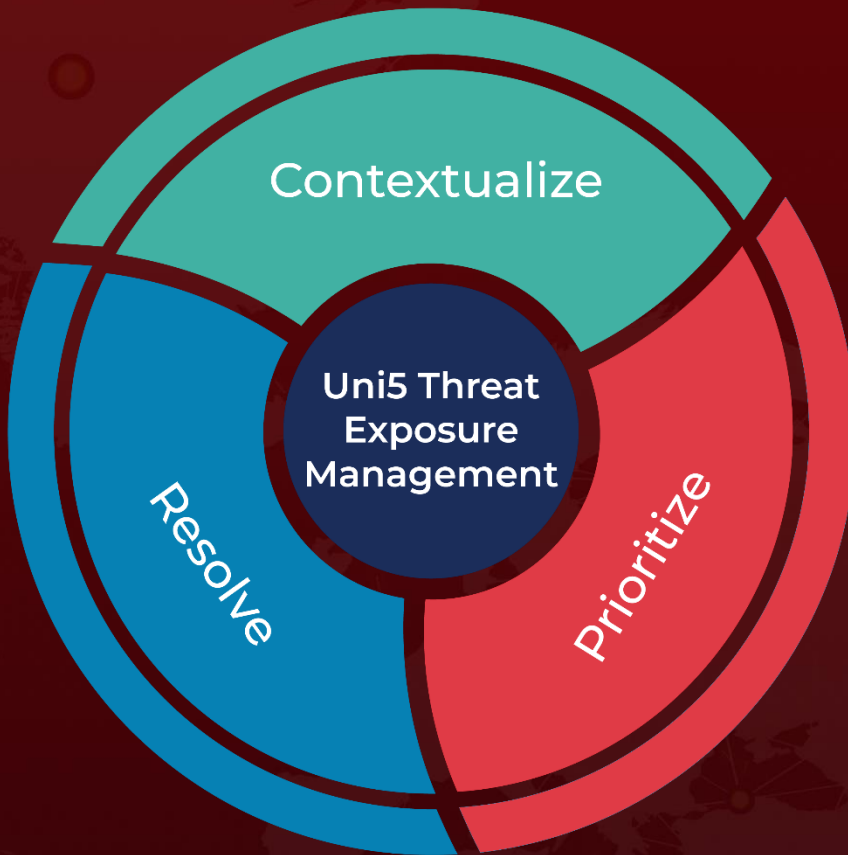
## References

<https://sansec.io/research/magento-xml-backdoor>

# What Next?

At Hive Pro, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with HivePro Uni5: Threat Exposure Management Platform.



REPORT GENERATED ON

**April 8, 2024 • 9:30 PM**

© 2024 All Rights are Reserved by Hive Pro



More at [www.hivepro.com](http://www.hivepro.com)