SECURITY ALERT

Cyber Defense Intelligence

February 22, 2022

SECURITY ALERT: Critical RCE bug in Adobe Commerce, Magenta

Overview:
On February 18, 2022, Adobe released a patch for CVE-2021-24086 that fixes an RCE bug in the Magento Open Source and Adobe Commerce platforms. The zero-day vulnerability was under active attack last weekend, resulting in Adobe releasing an emergency patch. Discovered by Eboda and Blaklis, CVE-2021-24086 is an arbitrary code execution vulnerability.

This week, researchers at Positive Technologies bypassed the patch for CVE-2021-24086 and reproduced the exploit. The new exploit, now tracked as CVE-2022-24087, is an elevation of privilege vulnerability in the Azure IoT CLI extension.

If an attacker is successful, he could deploy malicious code on a website and attain un-authenticated admin-level privileges. CVE-2022-2487 has a rating of 9.8 on the CVSS vulnerability-scoring system and unlike CVE-2022-24086 (which has limited attacks), has not been exploited in the wild. In Adobe's update, the company stated that they are aware of the vulnerability, and they've released an update for these versions of Adobe Commerce and Magento

Open Source:
2.3.3-p1 - 2.3.7-p2
2.4.0 - 2.4.3-p1.

Although Positive Technologies was able to successfully reproduce CVE-2021-24086, they have yet to share proof-of-concept (PoC) for the exploit with the public.

The Positive Technologies team stated that a web application firewall (WAF) won't help defend against attacks due to the various ways one can leverage the RCE bug. This kind of issue is extremely useful for threat actors looking to skim data from online stores (credit cards).

How Pillar Technology Partners is Protecting our Customers:

We offer EDR endpoint protection through Sophos and Microsoft Defender.

Sophos prevents threats and extends protection from the endpoint to beyond. Find threats and eliminate blind spots with autonomous, real time, index-free threat ingestion and analysis that supports structured, unstructured, and semi-structured data.

Pillar Technology Partners's Recommendations:
To resolve this vulnerability, Adobe recommends the following patches for CVE-2021-24087:
MDVA-43395 (must be applied first)
MDVA-43443 (must be applied on top of the first patch)

Indicators of Compromise (IoCs):

At this time, there are no known IoCs.

Other Helpful Resources:

- Past alerts and briefings from Pillar's Cyber Defense Intelligence Team
  - https://www.ptechcyber.com/intel-briefings
- Other resources on ptechcyber.com
  - https://www.ptechcyber.com/