UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

# CYBER GUIDANCE ISSUE 00245

## ZERO-DAY MAGENTO 2 ADOBE COMMERCE UNDER ATTACK

**DATE ISSUED:** 21st February 2022

| | | | |
|---|---|---|---|
| IMPACT | LOW | MEDIUM | **HIGH** |
| EASE OF EXPLOIT | HARD | **MEDIUM** | EASY |

## OVERVIEW

Discovered in the Magento 2 and Adobe Commerce platforms, this new Zero-day is under known active exploitation in the wild putting e-Commerce websites at risk from Magecart card skimming attacks and other problems prompting users to deploy emergency patches.

## BREAKDOWN

The issue stems from improper input validation and if the malicious actor had or managed to gain authenticated access with administrator privileges, they would be able to carry out a Remote Code Execution (RCE) attack. This security vulnerability has received a 9.8 / 10 CVSS score and is currently being tracked as CVE-2022-24086. Affected versions include 2.3.7-p2 and 2.4.3-p1 for both platforms. Magecart famously targets vulnerable versions of Magento, skimming credit card details of the purchaser on checkout. The group is made up of a number of sub-groups famous for credit card harvesting and is known to be constantly evolving and updating their practices and software tools to evade detection. Card skimming attacks have recently risen and are projected to continue to rise moving forward. See Cyber Guidance Issue 0072 & Cyber Guidance Issue 0075 for further examples and info.

## REMEDIATION STEPS

- If you are running Magento v2.3 or v2.4, deploy custom patches from Adobe
- If you are running Magento versions between 2.33 and 2.37 manually apply patches provided by Adobe
- If you are running Magento 2.3.3 or below you may not be vulnerable, however it is still recommended available patches be applied.

## REFERENCES & RESOURCES


| | |
|---|---|
| Adobe Commerce | https://support.magento.com/hc/en-us/articles/4426353041293-Security-updates-available-for-Adobe-Commerce-APSB22-12- |
| Threatpost | https://threatpost.com/adobe-zero-day-magento-rce-attack/178407/ |
| GitHub Gist | https://gist.github.com/wigman/171f9314d692d23330591d20cec3a9fd |