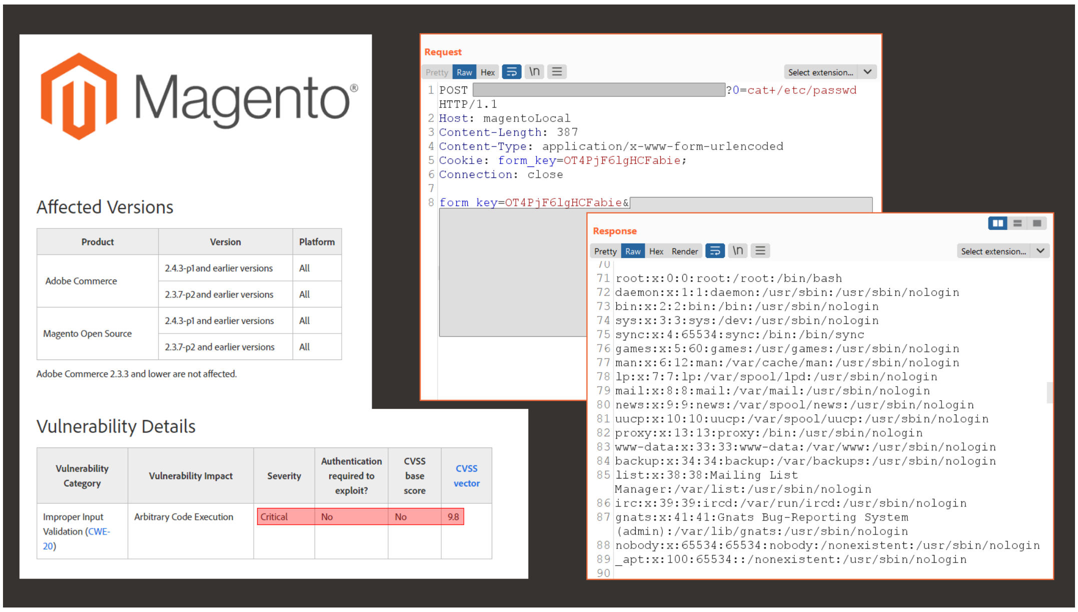
# Critical Remote Code Execution in Adobe Commerce, Magento: CVE-2022-24086 & CVE-2022-24087

A zero-day vulnerability in Adobe Systems Incorporated's Magento Open Source and Adobe Commerce was identified on February 13, 2022. CVE-2022-24086 adding a new issue that is now tracked as CVE-2022-24087, which has the same severity score and can lead to the same result when leveraged in attacks. Adobe Commerce versions 2.4.3-p1 (and earlier) and 2.3.7-p2 (and earlier) are affected by an improper input validation vulnerability during the checkout process. The exploitation of this issue does not require user interaction and could result in arbitrary code execution. The vulnerability scores 9.8 out of 10 on the CVSS vulnerability-severity scale, but there is one mitigating factor: An attacker would need to have administrative privileges in order to be successful.

Fig1. Positive Tecnologies



Affected Versions

| Product | Version | Platform |
|---|---|---|
| Adobe Commerce | 2.4.3-p1 and earlier versions | All |
| | 2.3.7-p2 and earlier versions | All |
| Magento Open Source | 2.4.3-p1 and earlier versions | All |
| | 2.3.7-p2 and earlier versions | All |

Adobe Commerce 2.3.3 and lower are not affected.

Vulnerability Details

| Vulnerability Category | Vulnerability Impact | Severity | Authentication required to exploit? | CVSS base score | CVSS vector |
|---|---|---|---|---|---|
| Improper Input Validation (CWE-20) | Arbitrary Code Execution | Critical | No | No | 9.8 |

```
POST [redacted]?0=cat+/etc/passwd
HTTP/1.1
Host: magentoLocal
Content-Length: 387
Content-Type: application/x-www-form-urlencoded
Cookie: form_key=OT4PjF6lgHCFabie;
Connection: close

form_key=OT4PjF6lgHCFabie&[redacted]
```

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List
Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System
 (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
```

Magento Open Source, formerly known as Magento Community. The free, open-source edition of Adobe Commerce is relatively potent and has many things to offer that are also included in the Adobe Commerce edition. This free environment is downloaded and tested thousands of times per month. It has a robust community of developers and evangelists and a codebase marketplace of tools and extensions that the community is thrilled to share.

## Explanation of the Vulnerability with its Impact

Improper Input validation is a common technique used to check potentially dangerous inputs to ensure that the inputs are safe for processing within the code or when communicating with other software components. When software fails to validate input properly, attackers are able to craft the malicious input in a form that is not expected by the rest of the application. This will lead to parts of the system receiving unintended input, resulting in altered control flow, arbitrary control of a resource, or arbitrary code execution.

A hacker can use arbitrary code execution to run a code or command on a target system by exploiting vulnerabilities. Remote code execution, on the other hand, allows a hacker to remotely execute arbitrary code on a target system or device by exploiting vulnerabilities. Once hackers have gained access to your website, they run arbitrary code to navigate and assess your files and find ways to gain full access to your website or application.

Since Magento and Adobe Commerce are very popular E-commerce platforms across the globe, this can potentially impact a high number of online shoppers. Moreover, the attack complexity needed to carry out a successful attack has been deemed relatively low/easy and no extra privileges/permissions are required to execute this attack. A successful attack can result in the total loss of confidentiality, integrity and availability of the information and resources stored in the exploited server.

## Explanation of the Exploit

The CVE-2022-24086 is about a remote code execution (RCE) without authentification. That brings hackers the opportunity to scan the internet for vulnerable sites and get full control over managing stores.

## Current Exploitation Status

Researchers from cybersecurity firm Sansec uncovered a massive Magecart campaign that already compromised more than 500 online stores running the Magento 1 eCommerce platform. Threat actors behind this campaign deployed a digital skimmer that was being loaded from the *naturalfreshmall(.)com* domain.

There is no threat group detected related to the CVE-2022-24086&CVE-2022-24087 for now.

## How to Mitigate CVE-2022-24086 & CVE-2022-24087?

Administrators of online stores running Adobe Commerce or Magento Open Source versions 2.4.3-p1/2.3.7-p2 and below are strongly advised to prioritize addressing CVE-2022-24086 and apply the update as soon as possible. Adobe Security, advises in order to stay up to date with the latest protections, customers must apply two patches: MDVA-43395 patch first, and then MDVA-43443 on top of it.

A Quick way to apply a patch;

```
> SSH into your server and cd into the Magento root directory.
> Create and edit a new file MDVA-43395.patch, insert the contents
  of the MDVA-43395_EE_2.4.3-p1_COMPOSER_v1.patch file from the
  archive above.
> Run “patch -p1 < MDVA-43395.patch”, or if that fails, run “patch
  -p2 < MDVA-43395.patch”.
> If you have OPCache running, try to flush it if you have the
  rights. Restarting your PHP service is also the way.
> Run “bin/magento cache:flush”.
```

The next step is to apply another patch for Magento 2: MDVA-43443. You have to install it on top of the last emergency patch .

## Conclusion

CVE-2022-24086 & CVE-2022-24087 vulnerabilities could result in arbitrary code execution. Adobe has released security updates for Adobe Commerce and Magento Open Source. These updates resolve a vulnerability rated critical. Successful exploitation could lead to arbitrary code execution. Adobe is aware that CVE-2022-24086 has been exploited in the wild in very limited attacks targeting Adobe Commerce merchants. Online store administrators are recommended to install the patches for both critical vulnerabilities to defend against exploitation attempts.

### References

1. Security updates available for Adobe Commerce - APSB22-12 (Adobe)
2. Security updates available for Adobe Commerce APSB22-12 (Adobe)
3. CVE-2022-24086 (MITRE)
4. CVE-2022-24087 (MITRE)
5. https://swissuplabs.com/blog/magento-2-critical-vulnerability-cve-2022-24086-see-the-way-to-fix-it/
6. https://support.magento.com/hc/en-us/articles/4426353041293-Security-updates-available-for-Adobe-Commerce-APSB22-12-
7. https://thesecmaster.com/what-is-arbitrary-code-execution/#:~:text=Arbitrary%20code%20execution%20allows%20a,system%2C%20usually%20from%20a%20WAN.
8. https://www.mend.io/vulnerability-database/CVE-2022-24087#:~:text=Date%3A%20January%2028%2C%202022,result%20in%20arbitrary%20code%20execution.

9. https://www.fortiguard.com/threat-signal-report/4419/active-exploitation-against-adobe-commerce-and-magento-through-cve-2022-24086-cve-2022-24087