April 9, 2024

Overall rating: Critical

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team is aware Adobe published security advisories to address vulnerabilities in multiple products. Included were updates for the following:

- Adobe Animate 2023 - version 23.0.4 and prior
- Adobe Animate 2024 - version 24.0.1 and prior
- Adobe Commerce - multiple versions
- Adobe Media Encoder - version 23.6.4 and prior
- Adobe Media Encoder - version 24.2.1 and prior
- Magento Open Source - multiple versions

Technical Details

Input validation is a frequently used technique for checking potentially dangerous inputs in order to ensure that the inputs are safe for processing within the code, or when communicating with other components. When software does not validate input properly, an attacker is able to craft the 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, which may result in altered control flow, arbitrary control of a resource, or arbitrary code execution.

Input validation is not the only technique for processing input, however. Other techniques attempt to transform potentially-dangerous input into something safe, such as filtering (CWE-790) - which attempts to remove dangerous inputs - or encoding/escaping (CWE-116), which attempts to ensure that the input is not misinterpreted when it is included in output to another component. Other techniques exist as well (see CWE-138 for more examples.)

- Input validation can be applied to:
    - raw data - strings, numbers, parameters, file contents, etc.
    - metadata - information about the raw data, such as headers or size

Exploitability Metrics
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None

This vulnerability is rated as a **CRITICAL** risk. A software update exists to address these risks.

Action Required

- Locate the device or application and investigate.
- Notify business owner(s).
- Perform mitigating actions, as required.

Please notify VRM with any questions or concerns you may have.

References

- CVE-2024-20758 CVE-2024-20759 CVE-2024-20772 CVE-2024-20797 CVE-2024-20795 CVE-2024-20796 CVE-2024-20794
- Adobe Security Advisory - APSB24-18
- Adobe Security Advisory - APSB24-23
- Adobe Security Advisory - APSB24-26
- Adobe Security Advisories