# НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru
E-mail: threats@cert.gov.ru

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20230315.1 | 15 марта 2023 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

## Выполнение произвольного кода в Adobe Commerce (formerly Magento Commerce)

| | |
|---|---|
| Идентификатор уязвимости | MITRE: CVE-2023-22247 |
| Идентификатор программной ошибки | CWE-91: Внедрение XML (внедрение XPath-кода вслепую) |
| Описание уязвимости | Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированных XML-данных. Уязвимость обусловлена некорректной проверкой входящих данных. |
| Категория уязвимого продукта | Прикладное программное обеспечение |
| Уязвимый продукт | Adobe Commerce (formerly Magento Commerce): 2.4.0 - 2.4.5-p1, 2.3.0 - 2.3.7-p4, 2.2.0 - 2.2.11, 2.0.0 - 2.0.18, 2.1.0 - 2.1.18<br>Magento Open Source: 2.4.0 - 2.4.5-p1, 2.3.0 - 2.3.7-p4, 2.2.0 - 2.2.11, 2.1.0 - 2.1.18, 2.0.0 - 2.0.18 |
| Рекомендации по устранению | Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков. |
| Дата выявления | 14 марта 2023 г. |
| Дата обновления | 14 марта 2023 г. |
| Оценка критичности уязвимости (CVSSv3.1) | 7.5 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N |
| Вектор атаки (AV) | Сетевой (N) |
| Сложность эксплуатации уязвимости (AC) | Низкая (L) |
| Необходимый уровень привилегий (PR) | Отсутствует (N) |

| | |
|---|---|
| Необходимость взаимодействия с пользователем (UI) | Отсутствует (N) |
| Масштаб последствий эксплуатации уязвимости (S) | Не изменяется (U) |
| Влияние на конфиденциальность (C) | Высокое (H) |
| Влияние на целостность (I) | Отсутствует (N) |
| Влияние на доступность (A) | Отсутствует (N) |
| Степень зрелости доступных средств эксплуатации | Не определено |
| Наличие средств устранения уязвимости | Официальное решение |
| Достоверность сведений об уязвимости | Не определено |
| Ссылки на источники | http://helpx.adobe.com/security/products/magento/apsb23-17.html |