

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20220124.24 | 24 января 2022 г.

Уровень опасности: **ВЫСОКИЙ**

Наличие обновления: **ЕСТЬ**

Выполнение произвольного кода в plugins XootiX for WordPress

| | |
|---|--|
| Идентификатор уязвимости | MITRE: CVE-2022-0215 |
| Идентификатор программной ошибки | Не определен |
| Описание уязвимости | Эксплуатация уязвимости позволяет удаленному злоумышленнику изменять произвольные параметры в уязвимом веб-приложении. Уязвимость обусловлена некорректной работой функции <code>save_setting</code> . |
| Категория уязвимого продукта | Прикладное программное обеспечение |
| Уязвимый продукт | easy-login-woocommerce: до 2.2 waitlist-woocommerce: до 2.5.2 side-cart-woocommerce: до 2.1 |
| Рекомендации по устранению | Обновить программное обеспечение |
| Дата выявления | 19 января 2022 г. |
| Дата обновления | 19 января 2022 г. |
| Оценка критичности уязвимости (CVSSv3.1) | 8.8 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N |
| Вектор атаки (AV) | Сетевой (N) |
| Сложность эксплуатации уязвимости (AC) | Низкая (L) |
| Необходимый уровень привилегий (PR) | Отсутствует (N) |
| Необходимость взаимодействия с пользователем (UI) | Требуется (R) |
| Масштаб последствий эксплуатации уязвимости (S) | Не изменяется (U) |
| Влияние на конфиденциальность (C) | Высокое (H) |
| Влияние на целостность (I) | Высокое (H) |

Влияние на доступность (A)

Высокое (H)

Степень зрелости доступных средств эксплуатации

Наличие не подтверждено

Наличие средств устранения уязвимости

Официальное решение

Достоверность сведений об уязвимости

Сведения подтверждены

Ссылки на источники

<https://www.wordfence.com/vulnerability-advisories/#CVE-2022-0215>