

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru

E-mail: threats@cert.gov.ru

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20200825.3 | 25 августа 2020 г.

Уровень опасности: **КРИТИЧЕСКИЙ**

Наличие обновления: **ЕСТЬ**

Множественные уязвимости в Discount Rules для WooCommerce plugin для WordPress

Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимый продукт	Discount Rules for WooCommerce: версии ПО 2.0.0, 2.0.1, 2.0.2
Дата выявления	20 июля 2020 г.
Дата обновления	20 июля 2020 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: N/A	<p>Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольные SQL-запросы к базе данных на целевой системе посредством отправки специально сформированных запросов к уязвимому приложению. Уязвимость обусловлена некорректной проверкой входных данных.</p> <p>CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C</p> <p>CWE-89: Некорректная нейтрализация специальных элементов, используемых в SQL-командах (внедрение SQL-кода)</p> <p>Рекомендации по устранению: обновить программное обеспечение.</p>	9.8

MITRE: N/A	<p>Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к уязвимому приложению на целевой системе посредством отправки специально сформированных сетевых пакетов. Уязвимость обусловлена некорректным функционированием компонента Ajax.</p> <p>CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N/E:U/RL:O/RC:C CWE-284: Некорректное управление доступом</p> <p>Рекомендации по устранению: обновить программное обеспечение.</p>	9.1
Ссылки на источники	https://www.webarxsecurity.com/multiple-vulnerabilities-in-discount-rules-for-woocommerce-plugin/	