НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200503.2| 3 мая 2020 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ОТСУТСТВУЕТ

Выполнение произвольных SQL-запросов в базе данных CMS PHP-Fusion

Идентификатор уязвимости	MITRE: CVE-2020-12461
Идентификатор программной ошибки	CWE-89: Некорректная нейтрализация специальных элементов, используемых в SQL-командах (Внедрение SQL-кода)
Описание уязвимости	Уязвимость позволяет удаленному злоумышленнику выполнять произвольные SQL-запросы в базе данных CMS PHP-Fusion. Уязвимость обусловлена недостаточной проверкой вводимых пользователем данных в maincore.php при обработке параметра «sort_order».
Категория уязвимого продукта	Серверное программное обеспечение и его компоненты
Уязвимое ПО	PHP-Fusion: 9.03.50
Рекомендации по устранению	На данный момент отсутствуют
Дата выявления	29 апреля 2020 г.
Дата обновления	29 апреля 2020 г.
Оценка критичности уязвимости (CVSSv3.1)	9.1 AV:N/AC:L/PR:N/UI:N/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)	Отсутствует (N)

Масштаб последствий эксплуатации уязвимости (S)	Не изменяется (U)
Влияние на конфиденциальность (C)	Высокое (H)
Влияние на целостность (I)	Высокое (H)
Влияние на доступность (A)	Низкое (N)
Степень зрелости доступных средств эксплуатации	Наличие не подтверждено
Наличие средств устранения уязвимости	Отсутствуют
Достоверность сведений об уязвимости	Сведения подтверждены
Ссылки на источники	https://github.com/php-fusion/PHP-Fusion/commit/79fe5ec1d5c75e017a6f42127741b9543658f822 https://github.com/php-fusion/PHP-Fusion/commit/858e43d7b0ea1897f76d5bcb3a1aed438132c0e2 https://github.com/php-fusion/PHP-Fusion/commit/d95cd4a2d22487723266c898b98e6be10754e03d https://github.com/php-fusion/PHP-Fusion/issues/2308 https://hackmd.io/lq7nA3ISSoeiGjiHVn5CoA https://www.cybersecurity-help.cz/vdb/SB2020050205