НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20210322.3 | 22 марта 2021 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Уязвимость в плагине Paid Memberships Pro для WordPress

Идентификатор уязвимости	MITRE: CVE-2021-20678
Идентификатор программной ошибки	CWE-89: Некорректная нейтрализация специальных элементов, используемых в SQL-командах (внедрение SQL-кода)
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному аутентифицированному злоумышленнику посредством отправки специально сформированного SQL-запроса получить несанкционированный доступ к базе данных WordPress. Уязвимость обусловлена из-за некорректной очисткой предоставленных пользователем данных.
Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимый продукт	Paid Memberships Pro: 2.0, 2.0.1, 2.0.2, 2.0.3, 2.0.4, 2.0.5, 2.0.6, 2.0.7, 2.1, 2.1.1, 2.1.2, 2.1.3, 2.1.4, 2.2, 2.2.1, 2.2.2, 2.2.3, 2.2.4, 2.2.5, 2.2.6, 2.3, 2.3.1, 2.3.2, 2.3.3, 2.3.4, 2.4, 2.4.1, 2.4.2, 2.4.3, 2.4.4, 2.5, 2.5.1, 2.5.2, 2.5.3, 2.5.4, 2.5.5
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	17 марта 2021 г.
Дата обновления	17 марта 2021 г.
Оценка критичности уязвимости (CVSSv3.1)	8.8 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
Вектор атаки (AV)	Сетевой (N)
Сложность эксплуатации уязвимости (AC)	Низкая (L)
Необходимый уровень привилегий (PR)	Низкий (L)
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)	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.cybersecurity-help.cz/vdb/SB2021031708 https://jvn.jp/en/jp/JVN08191557/index.html https://www.paidmembershipspro.com/pmpro-update-2-5-6/