НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200706.6| 6 июля 2020 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

SQL-инъекция в Payment Form плагина PayPal Pro для WordPress

Идентификатор уязвимости	MITRE: CVE-2020-14092
Идентификатор программной ошибки	CWE-89: Некорректная нейтрализация специальных элементов, используемых в SQL-командах (внедрение SQL-кода)
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольные SQL-запросы к базе данных приложения на целевой системе посредством отправки специально сформированных запросов. Уязвимость обусловлена некорректной обработкой входных данных.
Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимое ПО	Payment Form для PayPal Pro: 1.0.1, 1.0.2, 1.0.3, 1.0.4, 1.0.5, 1.0.6, 1.0.8, 1.0.9, 1.1.20, 1.1.21, 1.1.22, 1.1.23, 1.1.24, 1.1.25, 1.1.26, 1.1.27, 1.1.28, 1.1.29, 1.1.30, 1.1.31, 1.1.32, 1.1.33, 1.1.34, 1.1.35, 1.1.36, 1.1.37, 1.1.38, 1.1.39, 1.1.40, 1.1.41, 1.1.42, 1.1.43, 1.1.44, 1.1.45, 1.1.46, 1.1.47, 1.1.48, 1.1.49, 1.1.50, 1.1.51, 1.1.52, 1.1.53, 1.1.54, 1.1.55, 1.1.56, 1.1.57, 1.1.58, 1.1.59, 1.1.60, 1.1.61, 1.1.62, 1.1.63, 1.1.64, 1.2.48
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	2 июля 2020 г.
Дата обновления	3 июля 2020 г.
Оценка критичности уязвимости (CVSSv3.1)	9.8 AV:N/AC:L/PR:N/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)	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)	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/SB2020070304