НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200320.4 | 20 марта 2020 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Ошибка в контроле доступа в плагине Gutenberg & Elementor Templates Importer For Responsive для WordPress

Идентификатор уязвимости	Отсутствует
Идентификатор программной ошибки	CWE-284: Некорректное управление доступом
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному аутентифицированному злоумышленнику обойти ограничения безопасности и сбросить данные сайта, а также внедрить вредоносный код. Уязвимость обусловлена проблемами в разграничении доступа в различных действиях AJAX.
Категория уязвимого продукта	Серверное программное обеспечение и его компоненты
Уязвимое ПО	Responsive Add Ons: 1.0.0, 1.0.1, 1.0.2, 1.0.3, 1.0.4, 1.0.5, 1.0.6, 1.0.7, 2.0.0, 2.0.1, 2.0.2, 2.0.3, 2.0.4, 2.0.5, 2.0.6, 2.0.7, 2.0.8, 2.0.9, 2.1.0, 2.1.1, 2.2.0, 2.2.1, 2.2.2, 2.2.3, 2.2.4, 2.2.5
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	15 марта 2020 г.
Дата обновления	18 марта 2020 г.
Оценка критичности уязвимости (CVSSv3.0)	9.1 AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:H/A:L
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)	Изменяется (C)

Влияние на конфиденциальность (C)	Низкое (L)
Влияние на целостность (I)	Высокое (H)
Влияние на доступность (A)	Низкое (L)
Степень зрелости доступных средств эксплуатации	Концептуальное подтверждение
Наличие средств устранения уязвимости	Официальное решение
Достоверность сведений об уязвимости	Сведения подтверждены
Ссылки на источники	https://wpvulndb.com/vulnerabilities/10137/ https://www.wordfence.com/blog/2020/03/severe-flaws-patched-in-responsive-ready-sites-importer-plugin/