

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru

E-mail: threats@cert.gov.ru

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200327.3 | 27 марта 2020 г.

Уровень опасности: **ВЫСОКИЙ**

Наличие обновления: **ЕСТЬ**

Доступ к ограниченным функциям в плагине IMPress для IDX Broker в WordPress

Идентификатор уязвимости	MITRE: CVE-2020-9514
Идентификатор программной ошибки	CWE-284: Некорректное управление доступом
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному аутентифицированному злоумышленнику создавать и удалять «динамические страницы» посредством отправки специально созданного запроса в «wp-admin / admin-ajax.php». Уязвимость обусловлена некорректным ограничением доступа в действиях AJAX.
Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимое ПО	IMPress для IDX Broker до v2.6.2
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	26 марта 2020 г.
Дата обновления	27 марта 2020 г.
Оценка критичности уязвимости (CVSSv3.0)	8.1 AV:N/AC:L/PR:L/UI:N/S:U/C:N/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)	Отсутствует (N)
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.wordfence.com/blog/2020/03/vulnerabilities-patched-in-impress-for-idx-broker/>

<https://wpvulndb.com/vulnerabilities/10153/>