НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20201007.8 | 7 октября 2020 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Некорректная проверка криптографической подписи в плагине Microsoft Office 365 для WordPress

Идентификатор уязвимости	MITRE: CVE-2020-26511
Идентификатор программной ошибки	CWE-347: Некорректная проверка криптографической подписи
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевой системе посредством подделки JWT-токенов и обхода механизмов аутентификации и авторизации. Уязвимость обусловлена некорректной проверкой криптографической подписи.
Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимый продукт	WordPress + Office 365: 7.4, 7.8, 7.10, 7.11, 7.12, 7.13, 7.14, 7.17, 7.18, 8.1, 8.4, 8.5, 8.6, 9.0, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6, 10.0, 10.1, 10.3, 10.4, 10.6, 10.7, 10.9, 10.10, 11.0, 11.1, 11.3, 11.4, 11.6
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	2 октября 2020 г.
Дата обновления	2 октября 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)	Не требуется (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://wpvulndb.com/vulnerabilities/10418/ https://www.wpo365.com/change-log/