НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20220616.4 | 16 июня 2022 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Выполнение произвольного кода в Fortinet FortiDDoS

Идентификатор уязвимости	MITRE: CVE-2022-29060
Идентификатор программной ошибки	CWE-321: Использование жестко закодированного ключа шифрования
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику подписать JWT-токены для устройств посредством получения криптографического ключа с одного устройства. Уязвимость обусловлена использованием жестко запрограммированного криптографического ключа.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимый продукт	FortiDDoS версии с 5.5.0 по 5.5.1 FortiDDoS версии с 5.4.0 по 5.4.2 FortiDDoS версии с 5.3.0 по 5.3.1 FortiDDoS версии 5.2.0 FortiDDoS версии 5.1.0
Рекомендации по устранению	Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.
Дата выявления	07 июня 2022 г.
Дата обновления	07 июня 2022 г.
Оценка критичности уязвимости (CVSSv3.1)	7.8 AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
Вектор атаки (AV)	Сетевой (N)
Сложность эксплуатации уязвимости (AC)	Высокая (H)

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://fortiguard.fortinet.com/psirt/FG-IR-22-071