НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20190808.7 | 8 августа 2019 г.

Уровень опасности: СРЕДНИЙ

Межсайтовый скриптинг в WAF FortiWeb

Идентификатор уязвимости	MITRE: CVE-2019-5590
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код посредством отправки специально сформированной HTML-страницы. Уязвимость обусловлена недостаточной очисткой предоставленных пользователем данных при отображении элементов отчета об атаке.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимые системы и программное обеспечение	Fortinet FortiWeb: 6.0.0, 6.0.1, 6.0.2
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	12 июня 2019 г.
Дата обновления	12 июня 2019 г.
Оценка критичности уязвимости (CVSSv3)	6.3 AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:N/E:U/RL:O/RC:C
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)	Изменяется (C)
Влияние на конфиденциальность (C)	Низкое (L)
Влияние на целостность (I)	Низкое (L)
Влияние на доступность (A)	Отсутствует (N)

Степень зрелости доступных средств эксплуатации (E)	Наличие не подтверждено (U)
Наличие средств устранения уязвимости (RL)	Официальное решение (O)
Достоверность сведений об уязвимости (RC)	Сведения подтверждены (C)
Ссылки	https://www.cybersecurity-help.cz/vdb/SB2019061301?affChecked=1 https://www.securityfocus.com/bid/108786/info https://fortiguard.com/psirt/FG-IR-19-070