

# НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР  
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20221125.13 | 25 ноября 2022 г.

Уровень опасности: **ВЫСОКИЙ**

Наличие обновления: **ЕСТЬ**

## Выполнение атак XSS в Fortinet FortiManager и FortiAnalyzer

Идентификатор уязвимости	MITRE: CVE-2022-39950
Идентификатор программной ошибки	CWE-79: Некорректная нейтрализация входных данных при генерировании веб-страниц (межсайтовое выполнение сценариев)
Описание уязвимости	Эксплуатация уязвимости позволяет аутентифицированному удаленному злоумышленнику выполнить атаку с межсайтовыми сценариями (XSS) посредством открытия пользователем специально созданного вредоносного веб-сайта. Уязвимость обусловлена некорректной очисткой пользовательских данных в шаблонах отчетов.
Категория уязвимого продукта	Средства защиты информации
Уязвимый продукт	FortiAnalyzer: 7.0.0 - 7.0.4, 6.4.0 - 6.4.8, 6.2.0 - 6.2.9, 6.0.0 - 6.0.11 FortiManager: 7.0.0 - 7.0.4, 6.4.0 - 6.4.8, 6.2.0 - 6.2.9, 6.0.0 - 6.0.11
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	2 ноября 2022 г.
Дата обновления	2 ноября 2022 г.
Оценка критичности уязвимости (CVSSv3.1)	8.0 CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:H
Вектор атаки (AV)	Сетевой (N)

Сложность эксплуатации уязвимости (AC)	Низкая (L)
Необходимый уровень привилегий (PR)	Низкий (L)
Необходимость взаимодействия с пользователем (UI)	Требуется (R)
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	Не определено
Наличие средств устранения уязвимости	Официальное решение
Достоверность сведений об уязвимости	Не определено
Ссылки на источники	<a href="http://fortiguard.fortinet.com/psirt/FG-IR-21-228">http://fortiguard.fortinet.com/psirt/FG-IR-21-228</a>