

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20230220.2 | 20 февраля 2023 г.

Уровень опасности: **КРИТИЧЕСКИЙ**

Наличие обновления: **ЕСТЬ**

Обход пути в Weintek EasyBuilder Pro

Идентификатор уязвимости	MITRE: CVE-2023-0104
Идентификатор программной ошибки	CWE-22: Некорректные ограничения путей для каталогов (выход за пределы каталога)
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить доступ к конфиденциальной информации посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена некорректной проверкой входных данных при обработке последовательностей обхода каталогов.
Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимый продукт	EasyBuilder Pro: 6.07.01 - 6.08.01.349
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	20 февраля 2023 г.
Дата обновления	20 февраля 2023 г.
Оценка критичности уязвимости (CVSSv3.1)	9.3 CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:N/A:N
Вектор атаки (AV)	Сетевой (N)
Сложность эксплуатации уязвимости (AC)	Низкая (L)
Необходимый уровень привилегий (PR)	Отсутствует (N)
Необходимость взаимодействия с	Требуется (R)

пользователем (UI)

Масштаб последствий эксплуатации уязвимости (S)

Изменяется (C)

Влияние на конфиденциальность (C)

Высокое (H)

Влияние на целостность (I)

Отсутствует (N)

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

<http://ics-cert.us-cert.gov/advisories/icsa-23-045-01>