

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru

E-mail: threats@cert.gov.ru

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20210423.8 | 23 апреля 2021 г.

Уровень опасности: **ВЫСОКИЙ**

Наличие обновления: **ЕСТЬ**

Выполнение произвольного кода в Delta Electronics CNCSoft-B

Идентификатор уязвимости	MITRE: CVE-2021-22664
Идентификатор программной ошибки	CWE-787: Запись за границами буфера
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе. Уязвимость обусловлена ошибкой границ памяти при обработке входных данных.
Категория уязвимого продукта	Серверное программное обеспечение и его компоненты
Уязвимый продукт	CNCSoft-B: 1.0.0.0, 1.0.0.1, 1.0.0.2, 1.0.0.3
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	21 апреля 2021 г.
Дата обновления	21 апреля 2021 г.
Оценка критичности уязвимости (CVSSv3.1)	8.8 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N
Вектор атаки (AV)	Сетевой (N)
Сложность эксплуатации уязвимости (AC)	Низкая (L)
Необходимый уровень привилегий (PR)	Отсутствует (N)
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

Наличие не подтверждено

Наличие средств устранения уязвимости

Официальное решение

Достоверность сведений об уязвимости

Сведения подтверждены

Ссылки на источники

<https://www.cybersecurity-help.cz/vdb/SB2021042148>
<https://ics-cert.us-cert.gov/advisories/icsa-21-110-05>