

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20201223.2 | 23 декабря 2020 г.

Уровень опасности: **ВЫСОКИЙ**

Наличие обновления: **НЕТ**

Выполнение произвольного кода в Schneider Electric EcoStruxure Control Expert

Идентификатор уязвимости	MITRE: CVE-2020-7560
Идентификатор программной ошибки	CWE-123: Запись произвольных данных в произвольную область
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем файла. Уязвимость обусловлена некорректной работой функции обработки файлов проекта APX.
Категория уязвимого продукта	Промышленное программно-аппаратное оборудование
Уязвимый продукт	EcoStruxure Control Expert: v14,1
Рекомендации по устранению	На данный момент отсутствуют
Дата выявления	14 декабря 2020 г.
Дата обновления	14 декабря 2020 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)	Низкий (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	Отсутствует
Достоверность сведений об уязвимости	Сведения подтверждены
Ссылки на источники	https://www.se.com/ww/en/download/document/SEVD-2020-343-01/