НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200512.3| 12 мая 2020 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: НЕТ

Выполнение произвольного кода в ПО CODESYS Control Runtime System Toolkit

Идентификатор уязвимости	MITRE: CVE-2020-6081
Идентификатор программной ошибки	CWE-345: Некорректная проверка достоверности данных
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально созданного вредоносного сетевого пакета. Уязвимость обусловлена некорректной проверкой подлинности данных в функционале "PLC_Task".
Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимое ПО	CODESYS Control Runtime System Toolkit v3.5.14.30
Рекомендации по устранению	На данный момент отсутствуют
Дата выявления	6 мая 2020 г.
Дата обновления	6 мая 2020 г.
Оценка критичности уязвимости (CVSSv3.1)	9.9 AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H
Вектор атаки (AV)	Сетевой (N)
Сложность эксплуатации уязвимости (AC)	Низкая (L)
Необходимый уровень привилегий (PR)	Низкий (L)
Необходимость взаимодействия с пользователем (UI)	Отсутствует (N)
Масштаб последствий эксплуатации уязвимости (S)	Изменяется (C)
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	Недоступно
Достоверность сведений об уязвимости	Сведения подтверждены
Ссылки на источники	https://talosintelligence.com/vulnerability_reports/TALOS-2020-1003