НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20200518.3 | 18 мая 2020 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в Opto 22 SoftPAC Project

Категория уязвимого продукта	Серверное программное обеспечение и его компоненты
Уязвимое ПО	PAC Project Basic до v9.6 PAC Project Professional до v9.6
Дата выявления	17 мая 2020 г.
Дата обновления	17 мая 2020 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2020-10612	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольные команды в уязвимом приложении. Уязвимость обусловлена некорректными настройками прав доступа при взаимодействием SoftPACAgent с SoftPACMonitor через сетевой порт 22000. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H/E:U/RL:O/RC:C CWE-284: Некорректное управление доступом Рекомендации по устранению: обновить программное обеспечение.	9.1

MITRE: CVE-2020-10616	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного .dll файла. Уязвимость обусловлена некорректной загрузкой библиотек DLL. CVSSv3.0: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-427: Неконтролируемый элемент пути поиска Рекомендации по устранению: обновить программное обеспечение.	8.8

Ссылки на источники	https://www.cybersecurity-help.cz/vdb/SB2020051516