НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20220624.4 | 24 июня 2022 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

НСД в Phoenix Contact Classic Line Industrial Controllers

Идентификатор уязвимости	MITRE: CVE-2019-9201
Идентификатор программной ошибки	CWE-306: Отсутствие аутентификации для критически важных функций
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевой системе. Уязвимость обусловлена отсутствие аутентификации
Категория уязвимого продукта	Промышленное программно-аппаратное оборудование
Уязвимый продукт	ILC 1x0: Все версии AXC 1050: 2700988 AXC 1050XC: 2701295 AXC 3050: 2700989 RFC 480S: 2404577 RFC 470S: 2916794 RFC 460R: 2700784 RFC 430 ETH: 2730190 RFC 450 ETH: 2730200 PC WORX SRT: 2701680 PC WORX RT BASIC: 2700291 FC 350 PCI ETH: 2730844 ILC 1x1: до 4.42 ILC 3xx: до 3.98
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	22 июня 2022 г.

Дата обновления	22 июня 2022 г.
Оценка критичности уязвимости (CVSSv3.1)	9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C
Вектор атаки (AV)	Сетевой (N)
Сложность эксплуатации уязвимости (AC)	Низкая (L)
Необходимый уровень привилегий (PR)	Отсутствует (N)
Необходимость взаимодействия с пользователем (UI)	Отсутствует (N)
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	http://www.cisa.gov/uscert/ics/advisories/icsa-22-172-05