НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20200319.9 | 19 марта 2020 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: НЕТ

Множественные уязвимости в WAGO e!COCKPIT

Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимое ПО	WAGO e!COCKPIT версии 1.6.1.5 и 1.6.0.7
Дата выявления (обновления)	11 марта 2020 г. (17 марта 2020 г.)

Идентификаторы		Описание уязвимости, ссылки на источники	Оценка CVSSv3.1
Уязвимость	Программная ошибка		
MITRE: CVE-2019-5158	CWE-20: Некорректная проверка входных данных	Эксплуатация уязвимости позволяет удаленному злоумышленнику понизить версию прошивки устройства, что приведет к эксплуатации уязвимостей старых версий прошивки, посредством запуска пользователем специально созданного файла установки обновления. Уязвимость обусловлена некорректной проверкой введенных пользователем данных в компоненты пакета обновления прошивки. Рекомендации по устранению: Официальное решение отсутствует. Рекомендуем ограничить доступ к уязвимому устройству средствами межсетевого экранирования или принять иные административные меры.	8.8

MITRE: CVE-2019-5159	CWE-73: Внешнее управление именем или путем файла	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством запуска пользователем специально созданного файла установки обновления. Уязвимость обусловлена некорректной проверкой пути или имени файлов, которые используются в операциях файловой системы. Рекомендации по устранению: Пользователи должны выполнять обновления прошивки через e! COCKPIT, используя учетные данные администратора, а не суперпользователя (root) для контроллера.	8.8

Ссылки на источники	https://www.cybersecurity-help.cz/vdb/SB2020031812 https://talosintelligence.com/vulnerability_reports/TALOS-2019-0951 https://talosintelligence.com/vulnerability_reports/TALOS-2019-0952