

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru

E-mail: threats@cert.gov.ru

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20220727.13 | 27 июля 2022 г.

Уровень опасности: **КРИТИЧЕСКИЙ**

Наличие обновления: **ЕСТЬ**

Множественные уязвимости в Rockwell Automation ISaGRAF Workbench

Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимый продукт	ISaGRAF Workbench: 6.0 - 6.6.9
Дата выявления	22 июля 2022 г.
Дата обновления	22 июля 2022 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2022-2464	<p>Эксплуатация уязвимости позволяет удаленному злоумышленнику загрузить и запустить произвольный файл в целевой системе посредством отправки специально сформированного HTTP-запроса. Уязвимость обусловлена некорректной проверкой входных данных при обработке последовательностей обхода каталогов.</p> <p>CVSSv3.0: AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H/E:U/RL:O/RC:C</p> <p>CWE-22: Некорректные ограничения путей для каталогов (выход за пределы каталога)</p> <p>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.</p>	8.3

MITRE: CVE-2022-2465	<p>Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена некорректной проверкой входных данных при обработке сериализованных данных.</p> <p>CVSSv3.0: AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:N/A:H/E:U/RL:O/RC:C</p> <p>CWE-502: Десериализация недоверенных данных</p> <p>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.</p>	9.6
-------------------------	---	-----

Ссылки на источники	http://ics-cert.us-cert.gov/advisories/icsa-22-202-03
---------------------	---