НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20220906.11 | 6 сентября 2022 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в PTC Kepware KEPServerEX

Категория уязвимого продукта	Серверное программное обеспечение и его компоненты
Уязвимый продукт	ThingWorkx Industrial Connectivity: все версии ThingWorkx Kepware Edge: 1.4 KEPServerEX: до 6.12 OPC-Aggregator: до 6.12 ThingWorkx Kepware Server: до 6.12 TOP Server: до 6.12 Industrial Gateway Server: до 7.612 KEPServer Enterprise: до 6.12
Дата выявления	1 сентября 2022 г.
Дата обновления	1 сентября 2022 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2022-2848	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы. Уязвимость обусловлена ошибкой границ памяти. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H/E:U/RL:O/RC:C	9.1

	CWE-122: Переполнение буфера в динамической памяти 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.	
MITRE: CVE-2022-2825	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе. Уязвимость обусловлена ошибкой границ памяти. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-121: Переполнение буфера в стеке 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.	9.8

Ссылки на источники	http://ics-cert.us-cert.gov/advisories/icsa-22-242-10