НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20230301.3 | 1 марта 2023 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в PTC ThingWorx Edge

Категория уязвимого продукта	Серверное программное обеспечение и его компоненты
Уязвимый продукт	ThingWorx Edge C-SDK: 2.2.12.1052 .NET-SDK: 5.8.4.971 ThingWorx Edge MicroServer (EMS): 5.4.10.0 ThingWorx Kepware Server: 6.12 ThingWorx Industrial Connectivity: все версии ThingWorx Kepware Edge: 1.5 KEPServerEX: 6.12 KEPServer Enterprise: 6.12 Industrial Gateway Server: 7.612
Дата выявления	27 февраля 2023 г.
Дата обновления	27 февраля 2023 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2023-0755	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе. Уязвимость обусловлена некорректной проверкой индекса массива. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8

	CWE-129: Некорректная проверка индекса массива 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-2023-0754	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированных данных. Уязвимость обусловлена целочисленным переполнением. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H CWE-190: Целочисленное переполнение или циклический возврат 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://www.cisa.gov/uscert/ics/advisories/icsa-23-054-01