НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20220211.2 | 11 февраля 2022 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в Siemens Industrial Products

Категория уязвимого продукта	Промышленное программно-аппаратное оборудование
Уязвимый продукт	SIMATIC ET 200SP Open Controller CPU 1515SP PC2: все версии SIMATIC S7-1200 CPU family: 4.5, 4.5.1 SIMATIC S7-1500 CPU: 2.9.2, 2.9.3 SIMATIC S7-1500 Software Controller: все версии SIMATIC S7-PLCSIM Advanced: все версии SIMATIC Drive Controller: до 2.9.4 SIMATIC TIM 1531 IRC: до 2.2
Дата выявления	11 февраля 2022 г.
Дата обновления	11 февраля 2022 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2021-37185 CVE-2021-37204	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы посредством отправки специально сформированных данных. Уязвимость обусловлена CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C CWE-672: Использование ресурса после окончания срока его действия или освобождения	7.5

	Рекомендации по устранению: обновить программное обеспечение	
MITRE: CVE-2021-37205	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы. Уязвимость обусловлена утечкой памяти. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C CWE-401: Некорректное освобождение памяти до удаления последней ссылки (утечка памяти) Рекомендации по устранению: обновить программное обеспечение	7.5

Ссылки на источники	https://www.cybersecurity-help.cz/vdb/SB2022021105 http://cert-portal.siemens.com/productcert/pdf/ssa-838121.pdf