НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20220719.6 | 19 июля 2022 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в SIMATIC eaSie Core Package

Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимый продукт	SIMATIC eaSie Core Package: до 22.00
Дата выявления	13 июля 2022 г.
Дата обновления	13 июля 2022 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2021-44221	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы посредством отправки специально сформированных данных. Уязвимость обусловлена некорректной проверкой входных данных. 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-20: Некорректная проверка входных данных 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.	7.5

MITRE: CVE-2021-44222	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевой системе посредством отправки специально сформированных запросов. Уязвимость обусловлена отсутствием проверки подлинности. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:N/E:U/RL:O/RC:C CWE-306: Отсутствие аутентификации для критически важных функций 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.	10.0

Ссылки на источники	http://cert-portal.siemens.com/productcert/pdf/ssa-580125.pdf