НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20220112.24 | 12 января 2022 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в Schneider Electric Easergy P5

Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимый продукт	Easergy P5: до 01.401.101
Дата выявления	12 января 2022 г.
Дата обновления	12 января 2022 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2022-22722	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевой системе. Уязвимость обусловлена использованием жестко заданных учетных данных в коде приложения. CVSSv3.0: AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-798: Использование жестко закодированных учетных данных Рекомендации по устранению: обновить программное обеспечение	7.5

MITRE: CVE-2022-22723	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированных данных. Уязвимость обусловлена ошибкой границ памяти. CVSSv3.0: AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-119: Выполнение операций за пределами буфера памяти Рекомендации по устранению: обновить программное обеспечение	8.8

Ссылки на источники	http://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2022-011-03 https://www.cybersecurity-help.cz/vdb/SB2022011209