

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru

E-mail: threats@cert.gov.ru

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20220914.3 | 14 сентября 2022 г.

Уровень опасности: **ВЫСОКИЙ**

Наличие обновления: **ЕСТЬ**

Множественные уязвимости в Siemens SINEC INS

| | |
|------------------------------|--|
| Категория уязвимого продукта | Серверное программное обеспечение и его компоненты |
| Уязвимый продукт | SINEC INS: до 1.0 SP2 |
| Дата выявления | 14 сентября 2022 г. |
| Дата обновления | 14 сентября 2022 г. |

| Идентификатор уязвимости | Описание уязвимости | Базовый уровень CVSS |
|--------------------------|---|----------------------|
| MITRE: CVE-2016-0701 | <p>Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевой системе. Уязвимость обусловлена некорректно реализованным обмен ключами DH.</p> <p>CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C</p> <p>CWE-200: Разглашение важной информации лицам без соответствующих прав</p> <p>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.</p> | 7.5 |

| | | |
|--|---|------------|
| <p>MITRE: CVE-2020-12762</p> | <p>Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного JSON-файла. Уязвимость обусловлена ошибкой границ памяти.</p> <p>CVSSv3.0: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C</p> <p>CWE-787: Запись за границами буфера</p> <p>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.</p> | <p>8.8</p> |
| <p>MITRE: CVE-2020-7793</p> | <p>Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы посредством отправки специально сформированных данных. Уязвимость обусловлена некорректной проверкой ввода.</p> <p>CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C</p> <p>CWE-185: Некорректные регулярные выражения</p> <p>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.</p> | <p>7.5</p> |
| <p>Ссылки на источники http://cert-portal.siemens.com/productcert/txt/ssa-637483.txt</p> | | |