НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20210917.3 | 17 сентября 2021 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Выполнение произвольных команд операционной системы в Siemens Siveillance OIS

Идентификатор уязвимости	MITRE: CVE-2021-31891
Идентификатор программной ошибки	CWE-78: Некорректная нейтрализация специальных элементов, используемых в системных командах (внедрение команд ОС)
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольные команды в операционной системе посредством отправки специально сформированных запросов. Уязвимость обусловлена некорректной обработкой входящих данных.
Категория уязвимого продукта	Серверное программное обеспечение и его компоненты
Уязвимый продукт	Desigo CC: Все версии GMA-Manager: Все версии Operation Scheduler: Все версии Siveillance Control: Все версии Siveillance Control Pro: Все версии Siveillance OIS: до v2.5.3
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	16 сентября 2021 г.
Дата обновления	16 сентября 2021 г.
Оценка критичности уязвимости (CVSSv3.1)	9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Вектор атаки (AV)	Сетевой (N)
Сложность эксплуатации уязвимости (AC)	Низкая (L)
Необходимый уровень привилегий (PR)	Отсутствует (N)

Необходимость взаимодействия с пользователем (UI)	Отсутствует (N)
Масштаб последствий эксплуатации уязвимости (S)	Не изменяется (U)
Влияние на конфиденциальность (C)	Высокое (H)
Влияние на целостность (I)	Высокое (H)
Влияние на доступность (A)	Высокое (H)
Степень зрелости доступных средств эксплуатации	Наличие не подтверждено
Наличие средств устранения уязвимости	Официальное решение
Достоверность сведений об уязвимости	Сведения подтверждены
Ссылки на источники	https://www.cybersecurity-help.cz/vdb/SB2021091605 https://cert-portal.siemens.com/productcert/pdf/ssa-535380.pdf