НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200818.5| 18 августа 2020 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Выполнение произвольного кода в Siemens Desigo CC

Идентификатор уязвимости	MITRE: CVE-2020-10055
Идентификатор программной ошибки	CWE- 94: Некорректное управление генерированием кода (внедрение кода)
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированного вредоносного сетевого запроса. Уязвимость обусловлена некорректной проверкой входных данный при формировании отчетов компонентами BIRT.
Категория уязвимого продукта	Серверное программное обеспечение и его компоненты
Уязвимый продукт	Siemens Desigo CC: версии 3.x и 4.x Siemens Desigo CC Compact: версии 3.x и 4.x
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	12 августа 2020 г.
Дата обновления	12 августа 2020 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://cert-portal.siemens.com/productcert/pdf/ssa-786743.pdf https://www.cybersecurity-help.cz/vdb/SB2020081248