НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20220719.31 | 19 июля 2022 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: НЕТ

Множественные уязвимости в Siemens PADS Standard/Plus Viewer

Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимый продукт	PADS Standard/Plus Viewer: все версии
Дата выявления	14 июля 2022 г.
Дата обновления	14 июля 2022 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2022-34272 CVE-2022-34277 CVE-2022-34278 CVE-2022-34279 CVE-2022-34280 CVE-2022-34281	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного RCB-файла. Уязвимость обусловлена ошибкой границ памяти. CVSSv3.0: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:U/RC:C CWE-119: Выполнение операций за пределами буфера памяти Рекомендации по устранению: ограничить доступ к уязвимому продукту средствами межсетевого экранирования или другими административными мерами	8.8

MITRE: CVE-2022-34273 CVE-2022-34274 CVE-2022-34275 CVE-2022-34276 CVE-2022-34284 CVE-2022-34286 CVE-2022-34289	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена ошибкой границ памяти. CVSSv3.0: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:U/RC:C CWE-787: Запись за границами буфера Рекомендации по устранению: ограничить доступ к уязвимому продукту средствами межсетевого экранирования или другими административными мерами	8.8

Ссылки на источники	http://cert-portal.siemens.com/productcert/txt/ssa-439148.txt