НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20220426.7 | 26 апреля 2022 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в Elcomplus SmartPPT SCADA и SCADA Server

Категория уязвимого продукта	Промышленное программно-аппаратное оборудование
Уязвимый продукт	SmartPPT SCADA: 1.1 SmartPPT SCADA Server: 1.4
Дата выявления	20 апреля 2022 г.
Дата обновления	20 апреля 2022 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2021-43939	Эксплуатация уязвимости позволяет локальному аутентифицированному злоумышленнику повысить свои привилегии в целевой системе посредством отправки специально сформированных запросов. Уязвимость обусловлена некорректной авторизацией. CVSSv3.0: AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-285: Некорректная авторизация 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.	8.8

MITRE: CVE-2021-43934	Эксплуатация уязвимости позволяет удаленному злоумышленнику загрузить и выполнить вредоносный файл на уязвимом сервере. Уязвимость обусловлена некорректной проверкой файла во время загрузки. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-434: Отсутствие ограничений на загрузку файлов небезопасного типа 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.	9.8

Ссылки на источники	http://ics-cert.us-cert.gov/advisories/icsa-22-109-04 http://ics-cert.us-cert.gov/advisories/icsa-22-109-05