НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20220419.8 | 19 апреля 2022 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в Aethon TUG Home Base Server

Категория уязвимого продукта	Универсальные компоненты и библиотеки
Уязвимый продукт	TUG Home Base Server: до 24
Дата выявления	13 апреля 2022 г.
Дата обновления	13 апреля 2022 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2022-1066 CVE-2022-26423	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевой системе. Уязвимость обусловлена некорректной авторизацией. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:N/E:U/RL:O/RC:C CWE-862: Отсутствие авторизации 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.	8.2

MITRE: CVE-2022-1070	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить атаку типа «человек посередине». Уязвимость обусловлена возможностью доступа к конечной точке. 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-300: Возможность доступа к каналу из точки, не являющейся конечной (человек посередине) 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-22-102-05