НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20220812.27 | 12 августа 2022 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Выполнение произвольного кода в роутерах DrayTek Vigor

Идентификатор уязвимости	MITRE: CVE-2022-32548
Идентификатор программной ошибки	CWE-119: Выполнение операций за пределами буфера памяти
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированных данных. Уязвимость обусловлена ошибкой границ памяти.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимый продукт	Vigor 3910: до 4.3.1.1 Vigor 1000B: до 4.3.1.1 Vigor 2962: до 4.3.1.1 Vigor 2927: до 4.4.0 Vigor 2915: до 4.3.3.2 Vigor 2952: до 3.9.7.2 Vigor 2952P: до 3.9.7.2 Vigor 3220: до 3.9.7.2 Vigor 2926: до 3.9.8.1 Vigor 2862: до 3.9.8.1 Vigor 2620: до 3.9.8.1 Vigor 200n: до 3.9.8.1 Vigor 2133: до 3.9.6.4 Vigor 2762: до 3.9.6.4 Vigor 167: до 5.1.1 Vigor 130: до 3.8.5 VigorNIC 132: до 3.8.5 Vigor 165: до 4.2.4 Vigor 166: до 4.2.4 Vigor 2135: до 4.4.2

	Vigor 2765: до 4.4.2 Vigor 2766: до 4.4.2 Vigor 2832: до 3.9.6 Vigor 2865: до 4.4.0 Vigor 2866: до 4.4.0
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.
Дата выявления	5 августа 2022 г.
Дата обновления	5 августа 2022 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	http://www.trellix.com/en-us/about/newsroom/stories/threat-labs/rce-in-dratyek-routers.html