

Endgame Gear предупредила пользователей, что официальное ПО для настройки мыши OP1w 4k v2 распространяло вредоносное ПО. Проблема затронула файл, доступный на сайте компании с 26 июня по 9 июля. Сейчас заражённый файл удалён.

Вредоносная программа, обнаруженная внутри, называется Xred. Она: может похищать данные, управлять компьютером без ведома пользователя и загружать другие вирусы. Пока неясно, сколько пользователей пострадали.

Компания утверждает, что утечек данных не было, а взлома серверов не произошло. Уязвимость коснулась только страницы загрузки ПО для конкретной модели мыши. Все остальные источники, включая основной раздел загрузок на сайте, GitHub и Discord, остались чистыми.

Первым о проблеме сообщил пользователь Reddit, установивший программу с официального сайта и заметивший сбой в работе Windows. Это вызвало подозрения и последующую проверку.