Binarly обнаружила серьёзную уязвимость в UEFI-приложениях от производителя промышленной электроники DTResearch. Проблема затрагивает устройства, на которых работает технология Secure Boot — механизм, защищающий процесс загрузки системы.

Уязвимость получила код CVE-2025−3052. С её помощью злоумышленник может изменить специальные настройки в памяти NVRAM и обойти защиту Secure Boot. Это позволяет запускать вредоносный код до загрузки операционной системы, включая невидимые для антивирусов программы.

Особенность проблемы — в том, что уязвимое ПО подписано сертификатом Microsoft, что делает его «доверенным» для большинства систем. Microsoft уже выпустила защиту: добавила опасные файлы в чёрный список загрузки (DBX), чтобы они не запускались. Red Hat готовит аналогичное обновление.

DTResearch утверждает, что их ПО предназначалось только для устройств с UEFI от Insyde, где уязвимость не может быть использована из-за ограничений доступа к памяти. Однако эксперты считают, что в большинстве устройств на базе UEFI подобная атака всё же возможна.