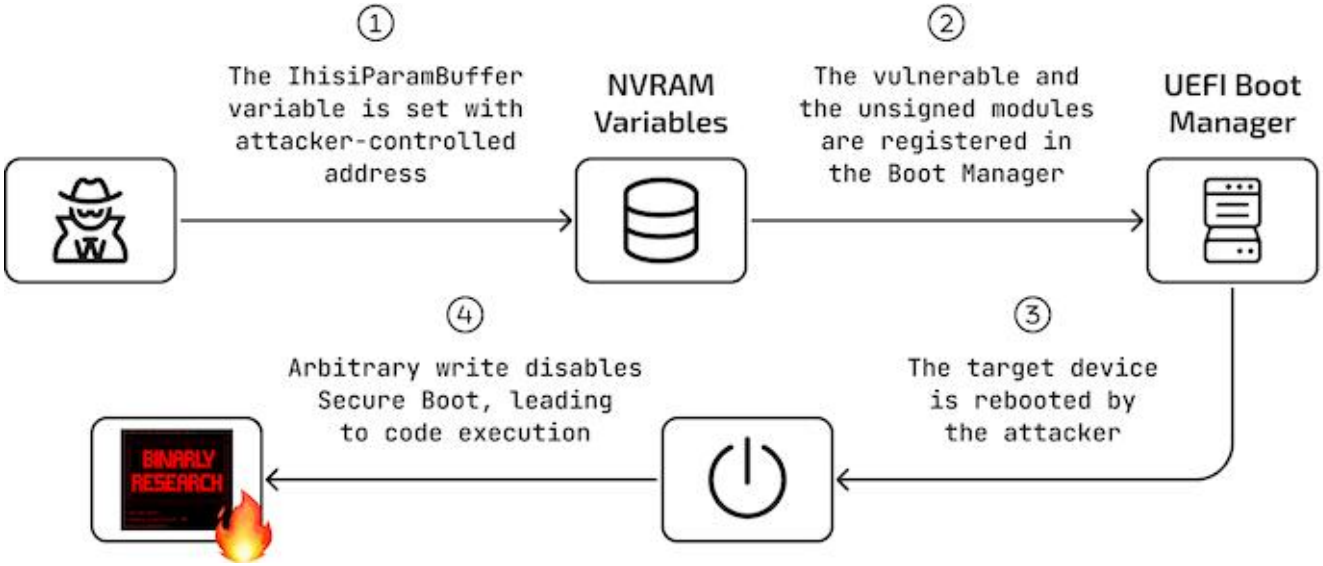
Исследователи из Binarly обнаружили серьёзную уязвимость в BIOS, позволяющую хакерам отключать Secure Boot и запускать вредоносный код ещё до загрузки Windows.

Проблема связана с UEFI-модулем, подписанным сертификатом Microsoft Third Party UEFI CA 2011, который используется на большинстве современных ПК.

Уязвимость позволяет через переменную «IhisiParamBuffer» внедрить вредоносный код без проверки, предоставляя злоумышленнику прямой доступ к памяти. Это открывает путь к установке bootkit-эксплойтов, которые загружаются с EFI-раздела и полностью обходят средства защиты на уровне ОС.

Microsoft уже выпустила обновление в рамках июньского Patch Tuesday, добавив уязвимые модули в список отзыва сертификатов (dbx).



HotHardware

Стоит отметить, что данное обновление критически важно: без него злоумышленник с админ-доступом может тихо отключить Secure Boot, обеспечив незаметную установку вредоносного ПО.

Пользователям рекомендуется как можно скорее установить актуальные обновления Windows и прошивок.