Новая уязвимость затрагивает сразу десять семейств процессоров популярного бренда.

Исследователи в области кибербезопасности выявили и описали новую уязвимость в прошивке Phoenix SecureCore UEFI (Unified Extensible Firmware Interface) – это интерфейс между операционной системой и микропрограммами, управляющими низкоуровневыми функциями оборудования компьютера. Он пришёл на смену устаревшего BIOS и представляет собой удобное в использовании, интуитивно понятное и поддерживающее ввод с помощью мыши программное обеспечение." data-html="true" data-original-title="UEFI" >UEFI, которая затрагивает несколько семейств настольных и мобильных процессоров Intel – американская корпорация, которая занимается производством широкого спектра электронных устройств и компьютерных компонентов, в частности микропроцессоры и наборы системной логики. Почти 100 % акций компании находится в свободном обращении на фондовых биржах.

 Корпорация Intel является одним из крупнейших в мире производителей микропроцессоров, который занимает 75% рынка. Среди основных клиентов компании выделяют производителей персональных компьютеров Dell и Hewlett-Packard. Помимо микропроцессоров, Intel также занимается выпуском полупроводниковых компонентов для промышленного и сетевого оборудования." data-html="true" data-original-title="Intel" >Intel.

Уязвимость, отслеживаемая как CVE-2024-0762 с оценкой CVSS 7.5, получила название «UEFIcanhazbufferoverflow». Она представляет собой переполнение буфера, возникающее из-за использования небезопасной переменной в конфигурации модуля TPM, что может привести к выполнению вредоносного кода.

Компания Eclypsium – это компания, занимающаяся кибербезопасностью. Она предлагает решения для защиты от вредоносного ПО и уязвимостей в аппаратных компонентах. Основные продукты Eclypsium включают в себя диагностику уязвимостей и мониторинг безопасности." data-html="true" data-original-title="Eclypsium" >Eclypsium, специализирующаяся на безопасности цепочек поставок, в своём отчёте отметила, что эта уязвимость позволяет локальному атакующему повысить привилегии и выполнить код в прошивке UEFI во время запуска.

Такого рода низкоуровневые эксплойты часто встречаются в случае бэкдоров в прошивке, подобных BlackLotus, которые становятся всё более распространёнными. Эти импланты дают атакующим постоянный доступ к устройству и возможность обходить более высокоуровневые меры безопасности, работающие в операционной системе и программном обеспечении.

Уязвимость CVE-2024-0762 затрагивает устройства с прошивкой Phoenix SecureCore, работающие на некоторых семействах процессоров Intel, включая AlderLake, CoffeeLake, CometLake, IceLake, JasperLake, KabyLake, MeteorLake, RaptorLake, RocketLake и TigerLake.

Уязвимость была устранена компанией Phoenix Technologies в апреле 2024 года, вскоре после ответственного раскрытия. Производитель персональных компьютеров Lenovo также уже выпустил обновления для устранения этой уязвимости в прошлом месяце.

UEFI, являющаяся преемником BIOS, представляет собой прошивку материнской платы, используемую при запуске для инициализации аппаратных компонентов и загрузки операционной системы через менеджер загрузки.

Факт того, что UEFI является первым кодом, запускаемым с наивысшими привилегиями, делает его привлекательной целью для злоумышленников, стремящихся внедрить буткиты и импланты прошивки, способные обойти меры безопасности и обеспечить длительное присутствие на устройстве без обнаружения.

Это также означает, что уязвимости, выявленные в прошивке UEFI, могут представлять серьёзную угрозу для цепочки поставок, так как они способны повлиять на множество продуктов и поставщиков одновременно.

Eclypsium подчеркнула, что прошивка UEFI является одним из наиболее ценных кодов на современных устройствах, и любая её компрометация может дать атакующим полный контроль и постоянный доступ к устройству.

Эти события произошли почти через месяц после того, как компания Eclypsium раскрыла аналогичную уязвимость переполнения буфера в реализации UEFI от HP, затрагивающую устройство HP ProBook 11 EE G1, которое было снято с производства в сентябре 2020 года.

Чтобы избежать компрометации, пользователям материнских плат с прошивкой от Phoenix Technologies рекомендуется следить за обновлениями UEFI на официальном сайте своей платы и обновить прошивку, как только исправление станет доступно.