Информационное сообщение ФСТЭК России от 25.10.2017 № 240/22/4900 "Об уязвимости микропрограммного обеспечения Intel Management Engine"

В октябре 2017 года выявлена уязвимость среднего уровня опасности в микропрограммном обеспечении Intel Management Engine (далее – Intel ME) версий 11.0 и выше, широко распространенном в средствах вычислительной техники государственных информационных систем и информационных систем персональных данных.

Указанная уязвимость позволяет нарушителю выполнить произвольный код в среде контроллера ввода-вывода (микросхема Platform Controller Hub) на материнских платах, предназначенных для центральных процессоров семейства Skylake и выше, в обход механизмов защиты, функционирующих на уровнях базовой системы ввода-вывода и операционной системы, и тем самым получить полный контроль над средством вычислительной техники.

Сведения об указанной уязвимости размещены в банке данных угроз безопасности информации (идентификатор уязвимости BDU:2017-02217).

Необходимо в обязательном порядке загрузить с официального сайта компании-разработчика и применить обновление, нейтрализующее указанную уязвимость (сведения о появлении указанного обновления будут размещены в банке данных угроз безопасности информации в поле «Информация об устранении» уязвимости BDU:2017-02217).

До применения указанного обновления необходимо принять следующие основные меры, направленные на исключение возможности эксплуатации уязвимости BDU:2017-02217:

1. Обеспечить защиту от несанкционированного физического доступа к аппаратным компонентам средств вычислительной техники.

2. Исключить каналы связи, обеспечивающие доступ в обход заданных правил управления доступом к средствам вычислительной техники(их программному обеспечению и настройкам), а также правил контроляи фильтрации информационных потоков.

3. Произвести отключение механизма удаленного управления средствами вычислительной техники Intel Active Management Technology (Intel AMT) путём применения соответствующих настроек базовой системы ввода-вывода.

4. Обеспечить защиту настроек базовой системы ввода-вывода от несанкционированного доступа путем применения пароля.

5. Обеспечить защиту от несанкционированного использования USB-портов средств вычислительной техники (в том числе при помощи их опечатывания, а также отключения путем применения соответствующих настроек базовой системы ввода-вывода).

6. Обеспечить ограничение установки (инсталляции) и исполнения в операционной системе программ в части установления возможности установки (инсталляции) и исполнения только программного обеспечения и (или) его компонентов в соответствии с разрешительными атрибутами безопасности.

Для информационных систем, имеющих подключение к иным информационным системам и информационно-телекоммуникационным сетям, также необходимо дополнительно принять следующие меры, направленные на нейтрализацию угроз, связанных с удаленной эксплуатацией уязвимости BDU:2017-02217:

1. Обеспечить межсетевое экранирование периметра информационной системы при помощи межсетевых экранов типа «А» соответствующего класса защиты. При этом необходимо активировать функцию преобразования сетевых адресов, а также настроить контроль и фильтрацию сетевого трафика по разрешительным атрибутам безопасности, запретив при этом межсетевое взаимодействие по портам 623, 664, 5900, 16992, 16993, 16994 и 16995.

2. Обеспечить автоматизированное обнаружение действий в информационных системах, направленных на преднамеренный несанкционированный доступ к информации и специальные воздействия на неё, путем применения систем обнаружения вторжений уровня сети и уровня узла.

Начальник 2 управления
Д.Шевцов

техническая защита информации