Защита McAfee против уязвимости Microsoft CryptoAPI

Тематика: **IT и телекоммуникации**
Анонсы мероприятий

г. Москва

Дата публикации: 3.02.2020

Дата мероприятия / события: 3.02.2020

03.02.2020, г. Москва -- Заявление Microsoft о наличии в Windows CryptoAPI уязвимости с условным названием CVE-2020-0601 попало в заголовки многих новостей. Данная уязвимость с высокой степенью риска позволяет хакерам подделывать подписи и цифровые сертификаты. Злоумышленник может применить поддельные сертификаты с шифрованием на основе эллиптических кривых (ECC) для подписи вредоносных файлов, чтобы избежать обнаружения или активации предупреждений безопасности браузера в отношении конкретных имен хостов. В результате пользователь будет считать, что файл поступил из надежного источника, а цифровая подпись якобы доверенного поставщика развеет оставшиеся подозрения. Успешное проникновение в систему также позволит хакеру проводить атаки типа «человек по середине» и выполнять расшифровку конфиденциальной информации при обращении пользователя к скомпрометированному ПО.

Как сообщается, уязвимость CVE-2020-0601 присутствует в операционных системах Windows 10, Windows Server 2019 и Windows Server 2016. Патч Microsoft (см. ниже) устраняет указанную уязвимость, обеспечивая всестороннюю проверку ECC-сертификатов в Windows CryptoAPI.

После обнаружения проблемы в сети было опубликовано описание механизма эксплойта. Воспользовавшись этими инструкциями, любой злоумышленник сможет подписывать исполняемые файлы от имени третьей стороны. Кроме того, ошибка позволяет перехватывать и подделывать безопасные веб-подключения (HTTPS), а также создавать фальшивые подписи для файлов и сообщений электронной почты.

Подробная информация о том, как корпоративные решения McAfee обеспечивают защиту от этой уязвимости, представлена ниже, а также в статье базы знаний KB92322. В ходе дальнейших исследований эти решения могут быть дополнены дополнительными мерами и средствами безопасности. Следите за обновлениями статей.

Что можно предпринять, чтобы защититься от угрозы?
Данная ошибка имеет высокую степень критичности. Все пользователи уязвимых операционных систем должны установить патч безопасности, подготовленный компанией Microsoft.

Крупным организациям с циклом установки патчей 15, 30 или 60 дней следует сделать исключение и обновить свои ОС как можно раньше.

Патчи безопасности Microsoft доступны по ссылке. Это угроза является настолько серьезной, что Агентство национальной безопасности США выпустило специальную инструкцию по устранению проблемы с информацией о том, как обнаружить взлом, и призывом к специалистам ИТ установить патчи Microsoft в кратчайший срок. Агентство по кибербезопасности и безопасности инфраструктуры (CISA) при Министерстве внутренней безопасности США (DHS) также издало чрезвычайную директиву, чтобы оповестить государственный сектор и правительственные организации о необходимости срочного обновления ОС Windows.

Как McAfee обеспечивает защиту своих заказчиков?
Решения McAfee помогают обнаружить эксплойт в ваших системах и предотвратить его использование. А именно:

Решение для безопасности рабочих мест McAfee Endpoint Security (ENS)
Технология McAfee устраняет указанную уязвимость с помощью сигнатуры, настроенной для обнаружения файлов с поддельной подписью.
Сервис сбора информации об угрозах Threat Intelligence Service (TIE)
TIE поможет выявить подделку подписей файлов до установки патчей за счет сравнения данных фальшивых центров сертификации и уже запущенных в системе бинарных файлов с аналогичной подписью.

Платформа безопасности сети McAfee Network Security Platform (IPS)
Подписи NSP (комплект Emergency Signature версии 10.8.3.3) исключат возможность эксплойта благодаря блокировке подключений с сертификатами, подверженными уязвимости.

Веб-шлюз Web Gateway
Проверка подлинности подписи файла реализована в защите от вредоносного ПО веб-шлюза McAfee. Благодаря сканированию HTTPs в Web Gateway проверка подлинности сертификатов будет производиться не на конечных точках, а на уровне шлюза. Это позволит применить централизованную механику обработки HTTPS-сертификатов, без использования уязвимой функции.

McAfee MVISION EDR
MVISION EDR обнаруживает попытки использования уязвимости уже на пропатченных системах. Устройства, которые подверглись такой атаке, будут отображаться на панели управления Real Time Search (поиск в реальном времени) после отправки запроса через NSACryptEvents.

McAfee Active Response (MAR)
McAfee Active Response обнаруживает попытки эксплойта указанной уязвимости. Чтобы выявить устройства, которые подверглись такой атаке, заказчик может создать специальный коллектор в каталоге Active Response Catalog и выполнить соответствующий запрос с помощью Active Response Search. Пользователи McAfee Active Response (MAR) также могут направлять запросы в режиме реального времени через коллектор NSACryptEvents.

McAfee Enterprise Security Manager (SIEM)
Решение McAfee Enterprise Security Manager способно обнаружить попытки эксплойта уязвимости на пропатченных системах. Для этого в процессе обычного обновления контента создаются новые подписи для направления событий в SIEM. (Порядок настройки правил ESM описан в статье базы знаний).

Новые правила загружаются на контент-сервер вместе с идентификатором новой подписи и описаниями таких событий. Заказчики могут использовать их для вывода предупреждений.

Подробная информация о доступе к описанным решениям представлена в статье базы знаний KB92322. В ходе дальнейших исследований эти решения могут быть усовершенствованы дополнительными мерами и средствами безопасности. Статья базы знаний KB92322 будет пополняться новыми рекомендациями и выводами.

О компании:
McAfee — компания, обеспечивающая киберзащиту в пространстве (от устройства до облака). Опираясь на принципы сотрудничества и взаимодействия, специалисты McAfee создают корпоративные и потребительские решения, которые делают мир безопаснее.
Наша целостная, автоматизированная и открытая платформа безопасности и "облачный" подход к созданию решений безопасности позволят всем вашим продуктам сосуществовать и обмениваться информацией об угрозах в любой точке цифрового ландшафта. Здесь автоматизация сочетается с человеческим разумом, что позволяет более эффективно оптимизировать рабочие процессы. Ваша команда освободится от ненужной оперативной нагрузки. Мы поможем организовать безопасность на территории и в облаке с помощью единой системы управления. Все ваши продукты по безопасности адаптируются к новым угрозам и будут работать в синергии, в целях повышения защиты на протяжении всего жизненного цикла угроз.
http://www.mcafee.com