SHAREPOINT 2016 ODATA УЯЗВИМОСТЬ

Трафимук М.П.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Селезнев И.Л. – к.т.н.,доцент

В современном мире все большее количество услуг и сервисов предоставляется посредством сети Интернет, поскольку Интернет и, соответственно, все его ресурсы доступны повсеместно. Помимо описанных положительных сторон есть и отрицательные: доступность, стабильность и надежность зависят не от пользователя, а от владельца ресурса. Обеспечить максимальную стабильность – это первостепенная задача администратора ресурса, для выполнения которой необходимо знать возможные уязвимости и способы их устранения.

С течением времени все большее количество услуг и сервисов предоставляется посредством сети Интернет. Повсеместное распространение доступа к сети и ее ресурсам является основной причиной этого явления. Помимо положительных сторон этого явления есть и отрицательные моменты: доступность, стабильность и надежность зависят не от пользователя, а от владельца ресурса. Обеспечить максимальную стабильность – это первостепенная задача администратора ресурса, для выполнения которой необходимо знать возможные уязвимости и способы их устранения.

На сегодняшний день ключевые ресурсы сети Интернет являются достаточно устойчивыми к различного вида атакам, использующим уязвимости протоколов UDP и TCP, а также DNS-серверов и других широко используемых сущностей. Ранее использование недоработок в этих компонентах для реализации атак приводило к неприятным последствиям для владельцев и администраторов ресурсов сети Интернет. Ключевой идеей этих, устаревших на данный момент, атак является генерация и отправка больших потоков данных атакуемому ресурсу.

Многие люди используют инструменты, предоставляемые Google для создания и редактирования документов, так как эти ресурсы бесплатны и доступны, однако они не удовлетворяют требованиям безопасности и функциональности для средних и крупных компаний. Такие компании, как правило, используют платную продукцию других компаний, среди которых наиболее широко известна компания Microsoft. Корневым узлом в инфраструктуре инструментария Microsoft со схожим, но более широким функционалом является Microsoft SharePoint Server. Он используется во многих серверах на базе Microsoft IIS, которых на данный момент 41,5% в сети Интернет [1]. Соответственно, уязвимость в корневом узле является блокирующей уязвимостью для всех поддерживаемых сервисов.

В Microsoft SharePoint Server 2016, самом актуальном на сегодняшний день, существует уязвимость, унаследованная от библиотеки Microsoft.Data.OData, которая обрабатывает и разбирает входящие запросы на составляющие части, после чего передает обработанную версию далее для верификации и исполнения. Уязвимость заключается в том, что при использовании фильтра некоторые комбинации вызывают критическую ошибку при обработке запроса, вследствие чего процесс останавливается и в автоматическом режиме запускается снова. Однако в качестве защиты от дестабилизации сервера перезапуск процесса происходит только 10 раз. По истечении 10 перезапусков восстановить работу можно только при ручной обработке ошибки и перезагрузке всей системы.

Алгоритм атаки следующий:

1) Установить подключение по SSL,
2) Проверить доступность сервера,
3) Сформировать вредоносный пакет, ключевым элементом которого является строка “filter=true”+”+or+true”*N, где N>=6100,
4) Отправить пакет серверу,
5) Перейти к пункту 1.

Таким образом, используя всего один компьютер, можно сделать недоступным Microsoft SharePoint Server 2016 приблизительно за 5 минут; этого времени, как правило, достаточно для автоматического перезапуска процесса и подготовки к приему новых пакетов для всех 10 итераций, необходимых для приведения сервера в недоступное состояние. Ключевой и единственной проблемой реализации данной атаки является необходимость установки подключения по SSL, что, в свою очередь, требует наличия корректного логина и пароля. В результате атаки для внешнего наблюдателя сервер на любой HTTP запрос будет отправлять код ответа из 500 серии, как правило, код 503 или, в редких случаях, 500. На момент написания данной статьи эта уязвимость не имеет способов устранения, однако известна компании Microsoft под кодом CVE-2018-8269.

Список использованных источников:

5. December 2018 Web Server Survey [Электронный ресурс]. – Режим доступа: https://news.netcraft.com/archives/2018/12/17/