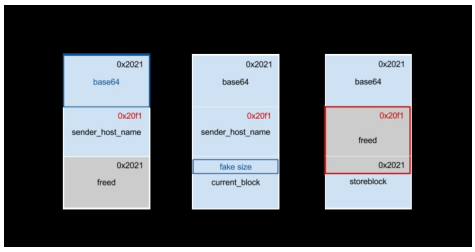
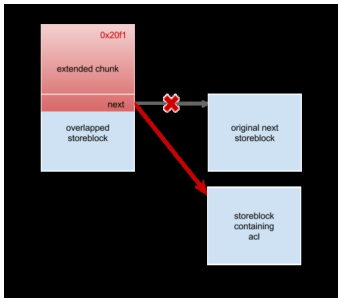
Автор:
07.03.18 19:26 -

Раскрыты детали техники эксплуатации уязвимости CVE-2018-6789, приводящей к однобайтовому переполнению в реализации декодировщика данных в формате BASE64, которая была устранена в начале февраля в выпуске Exim 4.90.1. Проблема проявляется при обработке данные в формате BASE64, размер которых не кратен 4 (4n+3). Рабочий эксплоит подготовлен для пакетов с Exim из состава Debian 9 и Ubuntu 17.04.

Изначально разработчики Exim скептически отнеслись к возможности практической эксплуатации проблемы, но выявивший уязвимость исследователь показал, что на основе данной уязвимости можно подготовить рабочий эксплоит, позволяющий выполнить код на сервере на стадии до прохождения аутентификации, отправив в качестве аргумента в команде "AUTH" специально оформленные данные в формате BASE64 и при помощи манипуляции с именем хоста отправителя в команде EHLO подготовив нужное смещение в куче для переопределения указателя на следующий блок памяти.



В итоге передачи определённой последовательности данных в командах "AUTH" и "EHLO" указатель на следующий блок хранения можно поменять и перенаправить на блок со строкой ACL. Таким образом, поступающие после команды AUTH данные будут записаны не в блок хранения, а в строку с ACL. Так как в ACL допускается использование конструкции "${run{cmd}}" для выполнения произвольных команд, можно переписать строку с ACL и организовать выполнение любой команды в момент проверки ACL.



Автор:
07.03.18 19:26 -

По оценке исследователя около 400 тысяч почтовых серверов на базе Exim подвержены риску быть атакованными. Всем администраторам рекомендуется убедиться, что на их системах используется Exim 4.90.1 или установлено обновление пакета с Exim от разработчиков дистрибутивов (Debian , FreeBSD , Ubuntu , Fedora , Arch Linux , openS
USE
,
SUSE
,
RHEL/EPEL
).

Read more http://www.opennet.ru/opennews/art.shtml?num=48219