системный администратор

системный администратор

№4(5) апрель 2003

подписной индекс 81655

журнал для системных администраторов, вебмастеров и программистов

Настройка RADIUS-сервера

Создаем VPN на основе vtun

Система фильтрации интернет-трафика

Компиляция FreeBSD

LIDS

Криптографическая защита информации

Продолжение исследования уязвимости в IIS (WebDAV)

Выпущенный патч против недавно обнаруженной уязвимости латает дырку в самом ядре операционной системы. Ее можно было использовать через переполнение, вызываемое WebDAV-запросом, однако это только один из способов. Сама проблема гораздо шире, чем может показаться, и касается не только серверов на IIS. NGSSoftware провела небольшое исследование, в результате которого были обнаружены и другие пути атаки.

В основе использования уязвимости по IIS-направлению лежало отсутствие ограничения на длину имени файла при WebDAV-запросе. При обработке этого запроса используются методы: PROPFIND, LOCK, SEARCH и GET с заголовком «Translate: f». Запрос проходит через несколько функций, одной из которых является GetFileAttributesExW. В свою очередь, из нее вызывается функция RtlDosPathNameToNtPathName_U, экспортируемая из ntdll.dll. Собственно, она и является основой проблемы.

RtlDosPathNameToNtPathName_U неправильно обрабатывает длину передаваемых строк. Неопределенные переменные являются 16-ти битными, следовательно, могут хранить значения от 0 до 65535. Если строка будет иметь длину 65536 байт, то будет считаться, что строка имеет длину 1, хотя реально она гораздо длиннее. Вот корень проблемы.

GetFileAttributesExW не единственная функция, вызывающая RtlDosPathNameToNtPathName_U, вот еще несколько: GetShortPathNameW, CopyFileW, MoveFileW, MoveFileExW, ReplaceFileW, CreateMailslotW, GetFileAttributesW, FindFirstFileExW, CreateFileW, GetVolumeInformationW, DeleteFileW, GetDriveTypeW, GetFileAttributesExW, CreateDirectoryW, FindFirstChangeNotificationW, GetBinaryTypeW, CreateNamedPipeW, SetFileAttributesW, MoveFileWithProgressW, GetVolumeNameForVolumeMountPointW, GetDiskFreeSpaceW, CreateDirectoryExW, DefineDosDeviceW, PrivMoveFileIdentityW, GetCompressedFileSizeW, SetVolumeLabelW, CreateHardLinkW, RemoveDirectoryW.

Как вы можете видеть, большинство функций используются для работы с файловой системой, атакующий может вызвать переполнение в любой из них, следовательно, все, что их использует, уязвимо. Но этим дело не заканчивается, ряд библиотек импортирует RtlDosPathNameToNtPathName_U из ntdll.dll, к ним относятся: acledit.dll, advapi32.dll, cscdll.dll, csrsrv.dll, dskquoui.dll, eventlog.dll, gdi32.dll, ifsutil.dll, lsasrv.dll, ntdll.dll, ntmarta.dll, ole32.dll, perfproc.dll, query.dll, rshx32.dll, scesrv.dll, sdbapiu.dll, setupdll.dll, sfc.dll, shell32.dll, shim.dll, srvsvc.dll, svcpack.dll, trkwks.dll, ulib.dll, wow32.dll.

Следовательно, существует достаточное количество вариантов проведения атаки, которые не обязательно должны касаться IIS, это могут быть и другие win32 веб, ftp, IMAP-сервера, антивирусное ПО и т. д.

Новый RFC кардинально решает проблему сетевых атак

Все гениальное, как всегда, просто – в протоколе IP v.4 достаточно незадействованных битов в поле флагов, один из которых предлагается использовать для отделения хакерских пакетов от обычных.

Вышел в свет эксплоит для ptrace

Данный эксплоит работает за счет проблемы с ptrace в ядре ОС Линукс. На данный момент не существует официального патча для линуксовых ядер, кроме как для версии 2.4.20, что делает проблему еще более актуальной.

Пример использования:

```
gcc kernelptrace.c .
/a.out
[+] Attached to 24983
[+] Waiting for signal
[+] Signal caught
[+] Shellcode placed at 0xccfd9ef0
[-] Unable to write shellcode: Input/output error
Killed
./a.out
[+] Attached to 24986
[+] Waiting for signal
[+] Signal caught
[+] Shellcode placed at 0xccfd9ef0
[-] Unable to write shellcode: Input/output error
Killed
./a.out
[+] Attached to 24989
[+] Waiting for signal
[+] Signal caught
[+] Shellcode placed at 0x4000e8fd
[+] Now wait for suid shell...
sh-2.05a#
```

Теперь о способах защиты. Именно от этого эксплоита поможет простое «chmod 700 /proc», так как этот эксплоит пытается открыть /proc/self/exe. Кроме того, можно воспользоваться модулем ядра, который расположен по адресу: http://www.austin2600.org/mirrors/004560.html.

Анализ ntdll.dll эксплоита для WebDAV

Эксплоит для NTDLL.DLL впервые был опробован на военном (military) сервере 17 марта сего года. Это было первое зарегистрированное использование «неопубликованного» эксплоита; Bugtraq лишь отчитался о ставшей известной уязвимости и о существующем эксплоите для неё. Это был случай, когда «незарелизенный» или «zero-day» эксплоит был использован для взлома до его публикации широким массам.

За серьезной проблемой в Microsoft's Internet Information Server (IIS) фактически стояла уязвимость в NTDLL.DLL, динамической библиотеке Windows, используемой всеми версиями Windows 2000, библиотеке, отвечающей непосредственно за работу с ядром системы. IIS web server – одно из множества приложений Windows 2000, использующих библиотеку NTDLL.

WebDAV расшифровывается как «Web-based Distributed Authoring and Versioning». И является расширением HTTP-протокола, позволяющим пользователям безопасно редактировать и управлять файлами на удаленном веб-сервере [wbdvorg].

После публикации в Bugtraq, CERT дал описание уязвимости и линк на патч от Microsoft. Windows 2000 предоставляет поддержку протокола WebDAV, который используется по умолчанию веб-сервером IIS. Пользователь, пославший специально сформированный HTTP-запрос на машину под IIS, может удаленно выполнять команды на сервере, в контексте IIS-сервиса.

MS классифицировала эту уязвимость как Critical.

RADIUS

ВСЕВОЛОД СТАХОВ