Использование специальных сигнатур сопоставления строк Cisco Secure IDS/NetRanger для предотвращения переполнения удаленного буфера червем Code Red в расширении ISAPI сервера Microsoft Index Server в IIS 4.0 и 5.0

Содержание

Введение

В конце июля 2003 Computer Economics (независимая исследовательская организация в Карлсбаде, Калифорния) оценила затраты корпораций на восстановление поврежденных сетей и потерь производительности, причиненных "Code Red", в 1.2 миллиардов долларов США. Эта оценка повысилась значительно с последующим релизом более мощного "Code Red II" червей. Система обнаружения несанкционированного доступа IDS Cisco, основной компонент Cisco SAFE Blueprint, продемонстрировала свое значение при обнаружении и снижении рисков сетевой безопасности, включая червя Code Red.

В настоящем документе описывается обновление программного обеспечения для определения метода эксплуатации, используемого червем Code Red (см. ниже Сигнатура 2).

Можно создать подписи соответствия пользовательской строки, которые, как показывают ниже, поймали эксплуатацию переполнения буфера для веб - серверы работающий с Microsoft Windows NT и информационные сервисы интернета (IIS) 4.0 или Windows 2000 и IIS 5.0. Также заметьте, что служба индексирования в бета-версии Windows XP также уязвима. Рекомендация по вопросам безопасности, которая описывает эту уязвимость, в http://www.eeye.com/html/Research/Advisories/AD20010618.html. Microsoft освободила исправление для этой уязвимости, которая может быть загружена от http://www.microsoft.com/technet/security/bulletin/MS01-033.mspx.

Подписи, обсужденные в этом документе, стали доступными в выпуске S (5) обновления подписи. Cisco Systems рекомендует, чтобы датчики были обновлены к 2.2.1.8 или 2.5 (1) обновление подписи S3 до реализации этой подписи. Зарегистрированные пользователи могут загрузить эти обновления подписи от Центра Программного обеспечения Cisco Secure. Все пользователи могут связаться со службой технической поддержки Cisco по электронной почте и телефону при помощи раздела международных контактов Cisco.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Сведения, содержащиеся в данном документе, взяты из следующих версий программного обеспечения:

- Microsoft Windows NT и IIS 4.0
- Microsoft Windows 2000 и IIS 5.0

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Технические рекомендации Cisco. Условные обозначения.

Подписи соответствия пользовательской строки

Существует две определенных подписи соответствия пользовательской строки для решения этой проблемы. Каждая подпись описана ниже, и параметры настройки применимого продукта предоставлены.

Подпись 1 вЂ” доступ к Index Server с попыткой злонамеренного использования

Эта подпись срабатывает при неудачном переполнении буфера на Сервере индексирования ISAPI расширения в сочетании с попытками передачи кода оболочки на сервер с целью получить привилегированный доступ к исходной форме кода. Подпись срабатывает только при попытке обойти код оболочки к целевому сервису для получения полного уровня доступа SYSTEM. Одна из возможных проблем состоит в том, что эта подпись не срабатывает, если хакер не пытается передать какой-либо код оболочки, а просто переполняет буфер, стремясь обрушить IIS и вызвать отказ в обслуживании.

Строка

```
[Gg][Ee][Tt].*[.][Ii][Dd][Aa][\x00-\x7f]+[\x80-\xff]
```

Параметры продукта

- Вхождения: 1
- Порт 80

Примечание: Если имеются веб-серверы, принимающие на других портах TCP (например, 8080), нужно создать отдельное соответствие пользовательской строки для каждого номера порта.

- Рекомендованный уровень важности сигнала тревоги:Высокий (Cisco Secure Policy Manager)5 (Unix Director)
- Направление:К

Подпись 2 — червь "Code Red" переполнения буфера доступа к серверу индексации

Вторая подпись стреляет в предпринятое переполнение буфера на Расширении сервера индексации ISAPI, объединенном с попыткой передать код оболочки к серверу для получения привилегированного адреса в запутываемой форме, которую использует Червь "Code Red". Эта подпись срабатывает только в попытку передать код оболочки к конечному сервису в попытке получить доступ уровня ВСЕЙ СИСТЕМЫ. Одна из возможных проблем состоит в том, что эта подпись не срабатывает, если хакер не пытается передать какой-либо код оболочки, а просто переполняет буфер, стремясь обрушить IIS и вызвать отказ в обслуживании.

Строка

```
[/]default[.]ida[?][a-zA-Z0-9]+%u
```

Примечание: В вышеупомянутой строке нет никаких пробелов.

Параметры продукта

- Вхождения: 1
- Порт 80

Примечание: Если имеются веб-серверы, принимающие на других портах TCP (например, 8080), нужно создать отдельное соответствие пользовательской строки для каждого номера порта.

- Рекомендованный уровень важности сигнала тревоги:Высокий (Cisco Secure Policy Manager)5 (Unix Director)
- Направление:К

Для получения дополнительной информации о Cisco Secure IDS обратитесь к Cisco Secure Intrusion Detection.

Дополнительные сведения

- Техническая поддержка - маршрутизаторы
- Сообщения Cisco Security

- Страница поддержки системы обнаружения несанкционированного доступа Cisco
- Техническая поддержка - Cisco Systems