Информационные сообщения и примечания по безопасности находятся на веб-узле http://www.cisco.com/go/psirt вместе с дополнительными сведениями группы реагирования на угрозы безопасности, связанные с уязвимостями решений (PSIRT).

Лучшие методы

Повышение уровня безопасности маршрутизаторов Cisco

Этот документ - неофициальное обсуждение некоторых настроек конфигурации Cisco, которые сетевым администраторам следует изменить на своих маршрутизаторах, особенно на граничных, для того чтобы улучшить безопасность. Данный документ содержит сведения о базовых, "шаблонных" элементах конфигурации, которые довольно широко используются в IP-сетях, а также о некоторых непредвиденных ситуациях, о которых также следует помнить.

Данные шифрования пароля Cisco IOS

Сторонний разработчик (не Cisco) выпустил программу для дешифрования паролей пользователей (и других паролей) в файлах конфигурации Cisco. **Программа не будет расшифровывать пароли, установленные с разрешением команды secret.** Непредвиденная проблема, которую данная программа вызвала у пользователей Cisco, вызвала подозрения, что многие пользователи полагаются на шифрование пароля Cisco как на средство большей безопасности, чем это было предусмотрено. В этом документе поясняется модель безопасности, на которой строится технология шифрования паролей Cisco, и особенности этого шифрования, ограничивающие безопасность

Cisco SAFE Blueprint
БЕЗОПАСНЫЙ проект универсальной безопасности, который позволяет организациям безопасно участвовать в электронной коммерции. Используя модульный подход, который упрощает разработку системы безопасности, развертывание и управление по мере роста и изменения сетей, SAFE дает дополнительные возможности сетям, построенным на основе Cisco AVVID (Архитектура для передачи голоса, видео и интегрированных данных).

Стратегии по защите от атак, их отслеживанию или подавлению

Описание и отслеживание лавинной передачи пакетов с помощью маршрутизаторов Cisco

> Атаки, провоцирующие отказ в обслуживании (DoS), распространены в Интернете. При такой атаке необходимо в первую очередь выяснить, к какому типу атак она относится. Часто атаки типа DoS связаны с насыщением интенсивным пакетным трафиком или иным потоком повторяющихся пакетов. В этом документе представлены более подробные сведения о данных атаках и способах их отслеживания.

Стратегии борьбы с вирусом Nimda

Этот индекс предоставляет всестороннюю распечатку всех практических советов и рекомендации смягчения для контакта с Вирусом nimda.

Стратегии борьбы с червём Code Red Worm

В алфавитном указателе содержится полный список технических рекомендаций и рекомендаций по уменьшению тяжести последствий в случае атаки червя Code Red.

Стратегии для защиты от атак Distributed Denial of Service (DDoS)

Это Описание технологических решений содержит техническое описание того, как потенциальный DDOS - атака происходит и предложенные методы для использования программного обеспечения Cisco IOS для защиты от него.

Стратегии защиты против атак на UDP-порт диагностики по типу "отказ в обслуживании"

Это Описание технологических решений содержит техническое описание того, как потенциальная Атака диагностического порта UDP происходит и предложенные методы для использования программного обеспечения Cisco IOS для защиты от него.

Стратегии защиты от атак типа "отказ в обслуживании" TCP SYN

Это Описание технологических решений содержит техническое описание того, как потенциальная Атака SYN TCP происходит и предложенные методы для использования программного обеспечения Cisco IOS для защиты от него.

Последнее в атаках "отказ в обслуживании": описание "Смурфинга" и информация для уменьшения эффектов
Примечание: Ссылка выше указывает на внешний сайт, который не поддерживается Cisco Systems, Inc.

Это предоставляет всестороннюю информацию относительно атак "smurf" с вниманием на маршрутизаторы Cisco и как уменьшить эффекты этих атак. Некоторая информация является общей и не связанной с конкретным предпочтительным поставщиком организации; однако, это записано с фокусом маршрутизатора Cisco. Этот документ не является подтверждением эффектов атак "smurf" на оборудование других поставщиков; однако, это действительно содержит информацию о различных поставщиках.

Другие ресурсы

Группа реагирования на угрозы безопасности, связанные с уязвимостями решений Cisco (PSIRT)

Этот документ содержит сведения по созданию отчета об ошибках и процедуры расследования инцидентов, в частности, что следует делать в случае активной атаки на безопасность сети или в случае угрозе такой атаке, при проблеме с безопасностью продукта Cisco, а также при появлении дополнительных вопросах об известной проблеме безопасности с продуктом Cisco. Роль Команды расследования инцидента, связанного с безопасностью продукта Cisco (PSIRT) в обработке случаев нарушения безопасности объяснена.