Введение

Увеличение зависимости человеческого общества от сетевых программных систем сопровождается увеличением количества нападений, совершаемых на эти системы. Такие нападения — направленные против правительств, корпораций, учебных заведений и частных лиц — приводят к потере и компрометации конфиденциальных данных, повреждению систем, потерям производительности и финансовым потерям.

Хотя многие из сегодняшних атак в Интернете — не более чем просто небольшое неудобство, существует все больше свидетельств того, что преступники, террористы и другие вредители ищут и используют уязвимости в программных системах для достижения своих целей. Сегодня скорость открытия уязвимостей программного обеспечения составляет свыше 4000 в год. Это вызвано проектированием и реализацией программного обеспечения, которые не защищают системы должным образом, и распространенной практикой программирования, когда программисты недостаточно сосредоточиваются на ликвидации дефектов реализации, которые приводят к появлению уязвимости.

Наблюдается также устойчивый прогресс в изощренности и эффективности атак злоумышленников, которые быстро разрабатывают вредоносные сценарии, использующие обнаруженные в программах уязвимости. Затем эти сценарии используются для несанкционированного доступа к информации, а взаимообмен такими сценариями способствует их широкому распространению. Эти сценарии в сочетании с программами, автоматически сканирующими сеть в поисках уязвимых систем, и их атаки приводят ко взрывообразному распространению нападений на вычислительные системы.

Большое количество обнаруживаемых каждый год уязвимостей приводит к перегруженности администраторов работой по исправлению существующих систем. Исправления для программ могут быть трудно применимыми или иметь неожиданные побочные эффекты. С того момента, когда разработчик выпускает обновление безопасности, и до момента его установки на 90–95% уязвимых компьютеров могут пройти месяцы или даже годы.

Ранее пользователи Интернета в значительной мере опирались на возможности интернет-сообщества в целом достаточно быстро реагировать на атаки на систему безопасности и сводить нанесенный ущерб к минимуму. Сегодня, однако, становится ясно, что мы

достигли пределов эффективности наших реактивных решений. Несмотря на все усилия отдельных организаций по рационализации и автоматизации процедур исправлений, количество уязвимостей в коммерческих программных продуктах в настоящее время находится на уровне, не позволяющем никаким, кроме самых обеспеченных любыми ресурсами, организациям идти в ногу с новыми исправлениями уязвимостей.

Имеется слишком мало свидетельств улучшений в области безопасности для большинства программных продуктов. Многие разработчики программного обеспечения не извлекают уроки из обнаруженных уязвимостей и не применяют надлежащие стратегии для смягчения последствий. Об этом свидетельствует тот факт, что CERT/CC[1] продолжает находить те же типы уязвимостей в последних версиях продуктов, которые имелись и в предыдущих версиях.

Взятые вместе, эти факторы указывают, что следует ожидать значительных экономических потерь от атак и сбоев в обслуживании даже при времени отклика, меньшем, чем мы можем реально надеяться достичь.

Агрессивный, скоординированный ответ по-прежнему необходим, но мы должны также строить более безопасные системы, взломать которые будет существенно сложнее.

О безопасном программировании на C и C++

В этой книге описаны основные ошибки при программировании на C и C++, которые приводят к наиболее распространенным, опасным и разрушительным уязвимостям программного обеспечения, зафиксированные со времени основания CERT в 1988 году. Эта книга обеспечивает как углубленный анализ инженерных программных ошибок, которые привели к таким уязвимостям, так и стратегии, которые могут быть эффективно применены для уменьшения или устранения риска использования этих уязвимостей злоумышленниками.

Я работаю с Робертом с апреля 1987 года, когда он впервые пришел в SEI[2]. Роберт — опытный инженер, который отлично зарекомендовал себя в области анализа уязвимостей программного обеспечения. Его книга предоставляет рецепты по разрешению наиболее распространенных проблем, стоящих перед разработчиками программного обеспечения, и предлагает практические решения. Обширный опыт Роберта в разработке программного обеспечения позволяет ему тонко чувствовать компромиссы между производительностью, удобством использования и другими свойствами программ, которые должны быть сбалансированы при разработке безопасного кода. В дополнение к способностям Роберта эта книга представляет знания, накопленные и отобранные командой анализа уязвимостей CERT/CC, а также вспомогательным персоналом SEI.

— Ричард Д. Петти (Richard D. Pethia)
Директор CERT

[1] Computer Emergency Response Team — команда "скорой компьютерной помощи" Института программной инженерии (SEI) Университета Карнеги-Меллон, экспертная группа реагирования на непредвиденные ситуации в компьютерных сетях. Выступает в роли наблюдателя за безопасностью в Интернете, круглосуточно консультирует по вопросам безопасности и защите от вирусов систем и данных в Интернете. Группа сформирована DARPA в ноябре 1988 года и финансируется государством. — *Примеч. пер.*

[2] Software Engineering Institute — Институт программной инженерии, научно-исследовательский центр, финансируемый Министерством обороны США, находится при Университете Карнеги-Меллон (г. Питтсбург, шт. Пенсильвания), имеет филиалы в штатах Алабама (г. Редстоунский Арсенал) и Виргиния (г. Арлингтон), а также в Германии (г. Франкфурт). — *Примеч. пер.*