Нарушения безопасности доступа к памяти: переполнения буфера, висячие указатели

Основы информационной безопасности

Андрианова М. Г.

18 октября 2024

Российский университет дружбы народов, Москва, Россия

Докладчик

- Андрианова Марина Геориевна
- студентка группы НПМбд-02-21
- Российский университет дружбы народов

Переполнение буфера

Переполнение буфера — запись за пределами выделенного в памяти буфера. Возникает при попытке записи в буфер блока данных, превышающего размер этого буфера. В результате переполнения могут быть испорчены данные, расположенные рядом с буфером, либо программа вовсе изменит своё поведение, вплоть до интерпретации записанных данных как исполняемого кода.

Причины возникновения

1. Недостаточная проверка входных данных.

2. Использование небезопасных функций.

3. Стековая и кучи.

4. Отсутствие защиты компилятора.

Последствия переполнения буфера

Переполнение буфера может иметь серьезные последствия для безопасности и стабильности программного обеспечения, включая:

1. Исполнение произвольного кода.
2. Утечка конфиденциальной информации.
3. Сбои и нестабильность системы.
4. Повреждение данных.
5. Увеличение уязвимости системы.

Висячие указатели

Висячий указатель (или “висячая ссылка”) — это указатель, который ссылается на область памяти, которая была освобождена или не существует. Возникает, когда объект был удалён (или перемещён), но значение указателя не изменили на нулевое. В данном случае он всё ещё указывает на область памяти, где находился данный объект. В некоторых случаях это может стать причиной получения конфиденциальной информации злоумышленником; либо, если система уже перераспределила адресуемую память под другой объект, доступ по висячему указателю может повредить расположенные там данные.

Причины возникновения:

Висячие указатели возникают по нескольким причинам:

- Освобождение памяти: Когда память выделяется динамически (например, с помощью malloc() или new), и после использования она освобождается, но указатель, ссылающийся на эту память, остается без изменений.
- Изменение объема памяти: При перераспределении памяти (например, с использованием realloc() в C) старый указатель может стать висячим, если не обновить его для указания на новый адрес выделенной памяти.
- Ошибки в логике программы: Ошибки в коде могут привести к тому, что указатели не обновляются или не обнуляются после освобождения памяти.

Последствия висячих указателей

Последствия использования висячих указателей могут быть серьезными и включать:

1. Сбой программы.
2. Непредсказуемое поведение.
3. Уязвимости безопасности.
4. Повреждение данных.

Защита от переполнения буфера

Существует несколько методов защиты от переполнения буфера, которые могут быть реализованы на уровне программирования, компиляции и операционных систем:

1. Использование безопасных функций.

2. Проверка границ.

3. Использование автоматического управления памятью.

4. Компиляция с защитными флагами.

5. Использование адресного пространства.

6. Использование стековых защитников.

Защита от висячих указателей

Для предотвращения проблем, связанных с висячими указателями, можно использовать следующие методы:

1. Обнуление указателей.

2. Управление памятью с помощью умных указателей.

3. Использование систем управления памятью.

4. Ведение учета выделенной памяти.

5. Проверка состояния указателей.

Заключение

- Понимание механизмов нарушений безопасности доступа к памяти, таких как переполнение буфера и висячие указатели, является критически важным для разработки надежного программного обеспечения. Эти уязвимости могут привести к серьезным последствиям, включая потерю данных, несанкционированный доступ к системам и выполнение произвольного кода.
- Обеспечение кибербезопасности требует комплексного подхода, который включает не только технические меры, но и обучение пользователей, политику безопасности и регулярный аудит систем. Технологии и методы, направленные на предотвращение уязвимостей, должны сочетаться с регулярными обновлениями программного обеспечения, мониторингом и анализом угроз.

Список литературы

- Джеймс Фостер, Майк Прайс. Защита от взлома: сокеты, эксплойты, shell-код = Sockets, Shellcode, Porting, & Coding. — М.: Издательский Дом ДМК-пресс, 2006. — С. 35, 532. — 784 с. — ISBN 5-9706-0019-9.
- Джон Эриксон. 0x320 Переполнение буфера // Хакинг: искусство эксплойта = Hacking: The Art of Exploitation. — 2-е издание. — СПб.: Символ-Плюс, 2010. — С. 139. — 512 с. — ISBN 978-5-93286-158-5.
- https://ru.ruwiki.ru/wiki/Безопасность_доступа_к_памяти#Типы_ошибок_памяти