

Buffer Overflow

Schwachstellen und wie man sie Schließt

Jakob Stühn, John Meyerhoff, Sam Taheri

H-BRS

November 26, 2021

- Eingabemöglichkeit
- Speichern der Eingabe
- Ablegen von Anweisungen durch übergroße Eingabe
- Ausführen der Anweisungen → Remote Code Execution

Anfälliger Quellcode

- Codebeispiel hier einfügen

Gegenmaßnahmen

Struktur

- Stack-Schutz mit “Canary” (Zufallszahl)
- Safe Pointer Instrumentalisierung
- C Range Error Detector und Out Of Bounds Object
- Hardware-basierte Lösungen
- Statische Code-Analyse
- Betriebssystembasierte Ansätze
- Manuelles Buffer-Overflow Blocken (Input-Bereinigung)

Gegenmaßnahmen

Code-Beispiel

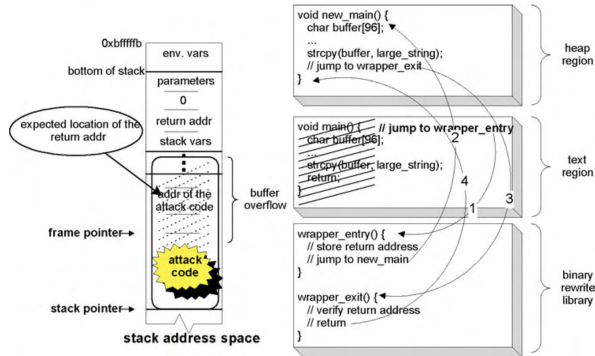


Figure 9: Libverify function call and stack layout

Gegenmaßnahmen

Testen

- Fuzzy Tests
- Spezifische Payloads

Quellen

- <https://www.nds.ruhr-unibochum.de/media/nds/attachments/files/2010/11/Survey.on.Buffer.Overflow.Attacks.ar>