Nanyang Technological University

AY2021-2022 Semester 2

# CE/CZ4067 SOFTWARE SECURITY

## Tutorial 5: Double Free and Shellshock

1. Double-free vulnerabilities occur when `free()` is called more than once with the same memory address as an argument. Recall from the lecture the double-free attack that follows a malloc-free-malloc-free pattern.

   - Allocate memory chunk `malloc(A)`;
   - Call `free(A)`, with forward consolidation to create a larger chunk;
   - Allocate a large chunk `malloc(B)`, hoping to get the space just freed;
   - Copy the ghost chunk into B at the location of A and a free ghost chunk adjacent to the chunk at A;
   - Call `free(A)` again, coalescing the two ghost chunks will try to remove the free ghost chunk from its bin.

   (a) Is the bin (i.e., double linked list) corrupted in the malloc-free-malloc-free exploit?

   (b) Which steps are deterministic? Where does the attacker need some luck to proceed?

2. An alternative double-free exploit is known as the free-free-malloc-malloc pattern. The steps are as follows.

   1. Prepare the memory into the layout shown in Fig. 1;
   2. Perform `free()` on the target chunk twice;
   3. Call `malloc()` with the size of the target chunk, and it may return the target chunk again;
   4. Legitimately write fake forward and backward pointers into the first eight bytes of the target chunk;
   5. Call `malloc()` with size of target junk, and hope to get the target chunk again; unlinking the target chunk will overwrite the memory.

   (a) What happens to the bin after Step 2?

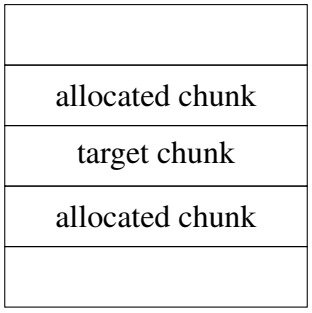


Figure 1: Memory layout after finishing Step 1.

(b) Why does the attacker prepare the memory layout such that the target chunk is surrounded by allocated chunks?

(c) What values should be written to the fake forward and backward pointers in order to perform a targeted overwrite?

(d) Which steps are deterministic? Where does the attacker need some luck to proceed?

3. Shellshock is a family of security bugs in the Unix Bash shell [1]. Shellshock could enable an attacker to cause Bash to execute arbitrary commands and gain unauthorized access [4] to many Internet-facing services, such as web servers, that use Bash to process requests. Collect information about Shellshock on the Internet (for example, [2, 3]), and answer the questions below.

(a) Find out more about the role of environment variables in the Shellshock vulnerability. Explain how the flaw in Bash shell allow an attacker to run arbitrary commands.

(b) Describe at least two example attack scenarios and discuss the potential impacts from the attacks.

# References

[1] What does the "Shellshock" bug affect? https://www.thesafemac.com/what-does-the-shellshock-bug-affect/, November 2021.

[2] Trend Micro. Bash vulnerability leads to Shellshock. https://www.trendmicro.com/en_us/research/14/i/shell-attack-on-your-server-bash-bug-cve-2014-7169-and-cve-2014-6271.html, November 2021.

[3] Trend Micro. Shellshock – how bad can it get? https://blog.trendmicro.com/trendlabs-security-intelligence/shellshock-how-bad-can-it-get/, November 2021.

[4] Larry Seltzer. Shellshock makes Heartbleed look insignificant. https://www.zdnet.com/article/shellshock-makes-heartbleed-look-insignificant/, November 2021.