Casper CTF: Solutions

Siebe Dreesen

1 Overview

2 Casper 4 solution

2.1 Description

This program takes 1 argument as input, if more are given it will print the first argument and stop the program immediately. The program contains a struct which contains a buffer of 775 characters and a function pointer. When less then 2 arguments are given the first will be copied into the buffer of the struct using strcpy() and the function pointer will be called. Normally this function pointer will point to the greetUser function which will print string.

2.2 Vulnerability

This program contains a memory management vulnerability, specifically a buffer overflow vulnerability. The struct contains a buffer and a function pointer which will be allocated under the buffer and the strcpy() which will copy the first argument does not do bounds checking. This means the buffer can be overflowed and the function pointer can be overwritten by giving an argument that is bigger than the allocated space for the buffer (775 bytes).

2.3 Exploit description

The vulnerability can be exploited by giving a well-chosen argument that is bigger than the buffer space and overwrites the function pointer. The argument contains shell code which will spawn the /bin/xh shell. The specific argument is build from the following bytes:

- A NOP sled of 755 bytes
- The shell code of 22 bytes
- Address of the sled which will be pointed to the shell code and overwrites the function pointer

2.4 Mitigation

3 Motivation

What is the gap in the literature? What is still missing? And why it is important? How can we envision the state of the art if the gap is filled?

4 Research Questions

Translate your motivations into specific research questions.

- RQ 1: ...
- RQ 2.1: ...
- RQ 2.2: ...
- ...

References

1. Author, F.: Article title. Journal **2**(5), 99–110 (2016)
2. Author, F., Author, S.: Title of a proceedings paper. In: Editor, F., Editor, S. (eds.) CONFERENCE 2016, LNCS, vol. 9999, pp. 1–13. Springer, Heidelberg (2016). https://doi.org/10.10007/1234567890
3. Author, F., Author, S., Author, T.: Book title. 2nd edn. Publisher, Location (1999)
4. Author, A.-B.: Contribution title. In: 9th International Proceedings on Proceedings, pp. 1–2. Publisher, Location (2010)
5. LNCS Homepage, http://www.springer.com/lncs. Last accessed 4 Oct 2017