Anthony Gimei

Cyber Security II (27465) WIIT-7420-03NI-27465-AU-2018

11/11/2018

Week 2 Assignment: CVE-2018-10718

Research your assigned CVE. Look for at least two sources of information about the vulnerability. One should be the vendor. Answer the following as best you can from the information you located:

Sources: <https://nvd.nist.gov/vuln/detail/CVE-2018-10718>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-10718>

<https://momo5502.com/blog/?p=34>

<https://vuldb.com/?id.117345>

1. What is your CVE number?

CVE-2018-10718

1. What is the CVSS score for the vulnerability?

Overall score of 10.0

1. Briefly describe the vulnerability:

“Stack-based buffer overflow in Activision Infinity Ward Call of Duty Modern Warfare 2 before 2018-04-26 allows remote attackers to execute arbitrary code via crafted packets.” - https://nvd.nist.gov/vuln/detail/CVE-2018-10718

1. What information are you able to find about the vulnerability?
   1. This is a buffer overflow vulnerability and has already been patched.
   2. An exploit that could be used for unpatched systems. Explanation on how to execute the exploit is here: <https://momo5502.com/blog/?p=34> and the code to execute the exploit here: <https://github.com/momo5502/cod-exploit>
2. What information does the vendor provide?

None

1. How do you exploit the vulnerability?

The vulnerability can be exploited by creating network packets that will construct a buffer overflow on the host system thereby making it possible for remote code execution on that host.

1. How difficult is it to use the exploit?

It is easy, one will need to be able to understand the application’s network protocol, and then find a way to replicate and modify the packets.

1. Can it be attacked externally (from the Internet) or only internally?

It can be attacked externally.

1. Do you require access (be authenticated) to the system, or not?

The CVE states that no privileges are required.

1. What is the mitigation for the vulnerability?

Upgrading the software mitigates the vulnerability.

1. How hard is it to apply the mitigation?

Upgrading the software is an easy process.

1. What risk does the mitigation present?

If a user does not upgrade then they are left vulnerable to attack

1. In your opinion, how much priority should be placed on mitigating your CVE?

High priority should be placed in mitigating this Vulnerability because it exposes the users host machine to an attacker being able to hijack the entire system and execute malicious software.