CALL OF DUTY: MODERN WARFARE 3 NULL POINTER DEREFERENCE

Luigi Auriemma[1] and Donato Ferrante[2]
ReVuln
http://revuln.com
info@revuln.com
http://twitter.com/revuln
13 November 2012

Abstract *In this paper we describe a pre-auth server-side NULL pointer dereference[3] vulnerability in Call Of Duty: Modern Warfare 3[4][5], which is due to an issue related to the DemonWare[6] query packets. This vulnerability can be exploited to perform Denial of Service (DoS) attacks against game servers.*

1 SOFTWARE DESCRIPTION

Call of Duty: Modern Warfare 3 (CoDMW3) is one of the most famous games available on multiple platforms (PC, Xbox360, PS3 and more). Its PC dedicated server is freely available on the Steam platform and is used by gaming server companies to rent servers for clans and casual players.

From Wikipedia[7]: "Within 24 hours of going on sale, the game sold 6.5 million copies in the U.S. and UK alone and grossed $400 million, making it the biggest entertainment launch of all time".

The vulnerability we are going to describe has been presented as a 0day for the first time during the Power of Community 2012 conference[8] in Seoul (*POC2012*). This advisory has been released publicly the 13th November 2012, just the same day in which Activision, the CoDMW3 publisher, released their latest title of the CoD series called *Call of Duty: Black Ops 2*.

2 VULNERABILITY DESCRIPTION

Just like its predecessor (CoDMW2) also this game relies on the DemonWare middleware for matchmaking capabilities and users authentication. The game uses the port 27015 as main UDP port, moreover all the UDP packets are encrypted and integrity checked.

[1] http://twitter.com/luigi_auriemma
[2] http://twitter.com/dntbug
[3] http://www.owasp.org/index.php/Null-pointer_dereference
[4] http://www.callofduty.com/mw3
[5] Version 1.9.453
[6] http://www.demonware.net
[7] http://en.wikipedia.org/wiki/Call_of_Duty:_Modern_Warfare_3
[8] http://www.powerofcommunity.net

The following is the format of the UDP packets (size 0x32 bytes):

- 32-bit *magic number*
- 32-bit *encryption init seed*
- *IPv4* address of the server
- *net_queryPort* of the server
- 8-bit DemonWare version (*0x02*)
- 8-bit *opcode*: *0x01* for *querysessioninfo* or *0x02* for *queryserverinfo*
- 64-bit query number (*random*)
- 64-bit query number (*random*)
- 32-bit *timestamp plus delta*
- public client *IPv4* address
- 64-bit xor'ed *MD5* hash
- 16-bit *CRC*

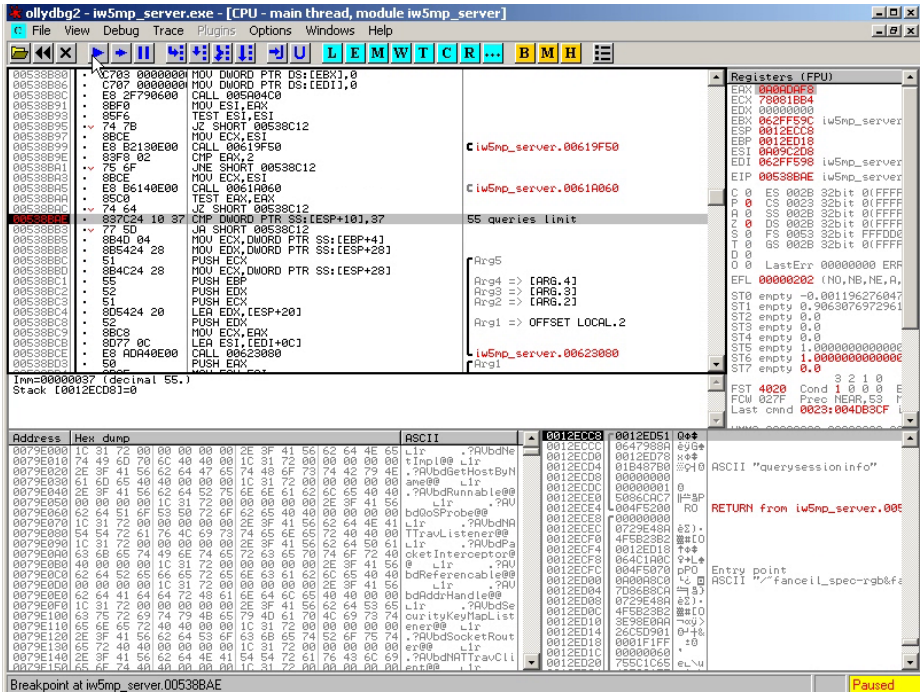

Figure 1: 55-query limit check

When the server receives a *querysessioninfo* or *queryserverinfo* packet, the server will forward the decrypted packet to the DemonWare master server. Please note

that this packet contains two 64-bit values that must be different from the values contained in the previous packets sent by the client. A valid DemonWare packet should have:

- correct *CRC*, *hash*, *net_queryPort* and *version*
- stored client IP address matching the public one of the client, so it must be the same of the source address
- *timestamp* within the *60 seconds range* expected by the server
- *random* query numbers
- random source port of the packets

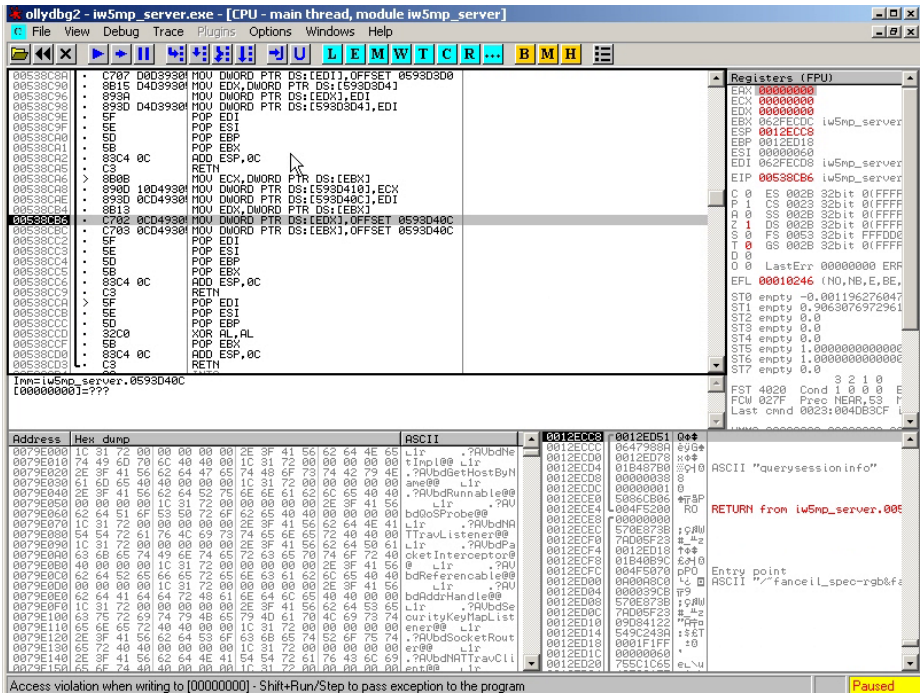

Figure 2: *NULL* pointer dereference

After 55 packets the server will crash due to a *NULL pointer dereference*. The UDP packets can be spoofed and the vulnerability affects both public and private servers. Please note that CoDMW3 public servers are listed online on the master servers, so an attacker may use this information to take down all the public servers at once.

One of the most common scenarios as explained during our talk at POC2012, is the one in which a competitor wants to ruin the business of the victim company, in order to steal their customers.

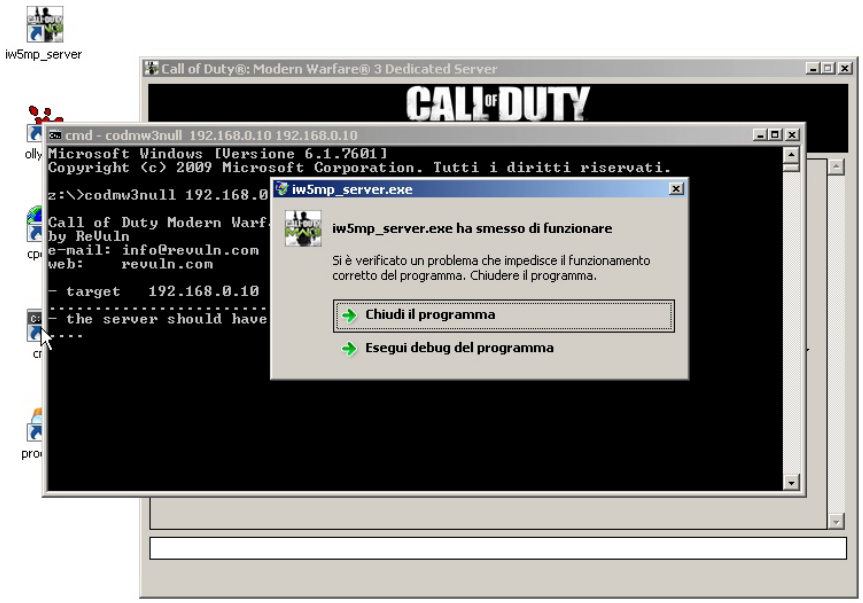

Figure 3: Denial of Service effects

3 Revision History

- 13 November 2012: Version 1.0 released.