CALL OF DUTY: MODERN WARFARE 3

NULL POINTER DEREFERENCE

Luigi Auriemma¹ and Donato Ferrante² 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 dereference³ vulnerability in Call Of Duty: Modern Warfare 3⁴⁵, which is due to an issue related to the DemonWare⁶ 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 Wikipedia⁷: "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 conference⁸ 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.

¹http://twitter.com/luigi_auriemma

²http://twitter.com/dntbug

³http://www.owasp.org/index.php/Null-pointer_dereference

⁴http://www.callofduty.com/mw3

⁵Version 1.9.453

⁶http://www.demonware.net

⁷http://en.wikipedia.org/wiki/Call_of_Duty:_Modern_Warfare_3

⁸http://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*

🔹 ollydbg2 - iw5mp_server.exe - [CPU - main thread, module iw5mp_server]		
C File View Debug Trace Plugins Options Windows Help		
HX F H H H H H H H H H H H H H H H H H H		
Dessessol Trops: 28:00 Dessessol Dessessol <thdessessol< th=""> <thdessessol< th=""> <</thdessessol<></thdessessol<>	<pre>CiuSnp_server.00619F50 CiuSnp_server.00619F50 S5 queries limit fhrg5 prg4 => [ARG.4] Arg3 => [ARG.2] Arg3 => OFFSET LOCAL.2 iuSnp_server.00623080 Fhrg1 </pre>	Besitter: (FPU) PARSILET: (FPU) PARSILET: (PARSILE) PARSILE: (PARSILE)
Address Hex dump ASCII	▲ 0312E008 0012ED51 00¢	10000-0000000-0000000-07
00779E0201 074 49 6D 70 6C 40 40 00 1C 31 72 00 00 00 00 00 01 10p0100 00779E020 25 87 41 56 62 64 47 65 74 46 6F 73 74 25 79 42 79 42 79 42 00779E020 50 61 50 65 40 40 00 00 1C 31 72 70 00 00 00 00 00 00 00 00 00 00 00779E020 00 40 56 65 65 75 70 66 66 66 66 60 62 66 74 40 74 00 00 00 00 00 00779E020 01 01 72 00 00 00 00 00 00 25 66 41 45 71 100 00 00 00 00 00 00 00 00 00 00 00 0	thossbyli 001255200 010000000 001000000 Lip 001255200 000000000 00000000 00000000 bef000 001255200 000000000 00000000 00000000 000000000 000000000 000000000 000000000 0000000000 0000000000 0000000000 0000000000 0000000000 0000000000 0000000000 00000000000 00000000000 000000000000 00000000000000000 000000000000000000000000000000000000	SCII "querysessioninfo" ETURN fron iu5mp_server.005 ntry point SCII "/"fanceil_spec-ryb&fi

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

🐱 ollydbg2 - iw5mp_server.exe - [CPU - main thread, module iw5mp_server]			
C File View Debug Trace Plugins Options Windows Help	_ 8 ×		
00538C8A • C707 D0D39300 MOU DWORD PTR DS:(EDI],OFFSET 0593D3D0 00538C90 • 8B15 D4D39300 MOU EDX,DWORD PTR DS:(593D3D4)	 Registers (FPU) 		
Session 201 Session Processed into Durch PTR Dist (EDX) (DI Session 201 Session Processed into Durch PTR Dist (EDX) (DI Session 201 Session Processed into Durch PTR Dist (EDX) (DI Session 201 Session Processed into Durch PTR Dist (EDX) (DI Session 201 Session Processed into Durch PTR Dist (EDX) (DI Session 201 Session Processed into Durch PTR Dist (EDX) (DI Session 201 Session Processed into Durch PTR Dist (EDX) (DI Session 201 Session Processed into Durch PTR Dist (EDX) (DI Session 201 Session Processed into Durch PTR Dist (EDX) (DI Session 201 Session Processed into Durch PTR Dist (EDX) (DI Session 201 Session Processed into Durch PTR Dist (EDX) (DI Session 201 CT33 BOD AND PTR Dist (EDX) (DI Session 201 CT33 BOD AND PTR Dist (EDX) (DIFFSET BESSID4GC) Session 201 CT33 BOD AND PTR Dist (EDX) (DIFFSET BESSID4GC) Session 201 Session Processed into Dist (EDX) (DIFFSET BESSID4GC) Session 201 Session Processed into Dist (EDX) (DIFFSET BESSID4GC) Session 201 Session 201 Session 201 Session 201 Session 201 Session 201	ERK Bedeleded ECK Bedeleded ECK Bedeleded ECK Bedeleded ECK Bedeleded ECK Bedeleded ECK Bedeleded EFK B		
Address Hex dump ASCII Image: Constraint of the state of	A 10000 000000 000000000000000000000000		
100756000 25 74 25 26 27 27 27 27 27 27 26 27	RECII "querysessioninfo" RETURN from iw5mp_server.005 Entry point RECII "/~fanceil_spec-rgb&fa		
Access violation when writing to [00000000] - Shift+Run/Step to pass exception to the program	Paused		

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.

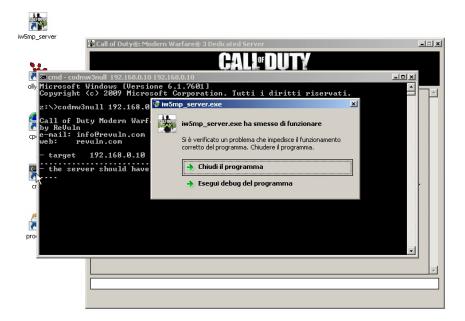


Figure 3: Denial of Service effects

3 REVISION HISTORY

• 13 November 2012: Version 1.0 released.