Doomsday Engine - Bug #473

Multiple Vulnerabilities - buffer overflow, DoS

2007-09-13 06:25 - draconx

Status:	Closed	**Start date:**	2007-09-13
Priority:	High	**% Done:**	100%
Assignee:	skyjake		
Category:			
Target version:	1.9.0-beta5		

Description

I poked through the latest SVN and this bug tracker and didn't see any sign of these being known about. They have lead to the package being masked on gentoo.

Source:
http://secunia.com/advisories/26524/

Luigi Auriemma has reported some vulnerabilities in Doomsday, which can be exploited by malicious people to cause a DoS (Denial of Service) or potentially compromise a vulnerable system.

1) A boundary error exists within the "D_NetPlayerEvent()" function in d_net.c when processing chat messages. This can be exploited to overflow a global buffer by sending an overly long chat message to the affected server.

Successful exploitation may allow the execution of arbitrary code on the game server and the connected clients.

2) A boundary error exists within the "Msg_Write()" function in net_msg.c when processing chat messages. This can be exploited to overflow a global buffer by sending an overly long chat message to the affected server.

3) An integer underflow error exists within the "Sv_HandlePacket()" in sv_main.c when processing chat messages. This can be exploited to trigger a failure to allocate required memory, which leads to a DoS.

4) A boundary error exists within the "NetSv_ReadCommands()" function in d_netsv.c when processing client commands. This can be exploited to overflow a static buffer by sending more than 30 commands to the affected server.

5) A format string error exists within the "Cl_GetPackets()" function when processing "PSV_CONSOLE_TEXT" messages sent by the server. This can potentially be exploited by a malicious server to execute arbitrary code on the affected clients by sending a specially crafted messages.

NOTE: An error in the processing of chat messages may leave a string without a NULL character at the end. This may trigger other vulnerabilities.

The vulnerabilities are reported in version 1.9.0-beta5.1 and prior. Other versions may also be affected.

Original Advisory:
http://aluigi.altervista.org/adv/dumsdei-adv.txt

Labels: Networking

History

#1 - 2007-09-15 14:38 - yagisan

Logged In: YES
user_id=1248824
Originator: NO

very overstated. I can't duplicate the so-called remote code execution - however it does DoS - I only found out about this around the time you posted here, so I'm very unhappy with the "contacted developers bit"

#2 - 2007-10-06 11:26 - yagisan

Logged In: YES
user_id=1248824
Originator: NO

I've fixed most of these - downgrading

#3 - 2007-11-22 07:40 - yagisan

Logged In: YES
user_id=1248824
Originator: NO

removing from self

#4 - 2008-07-05 20:25 - danij

Logged In: YES
user_id=849456
Originator: NO

Which (if any) of these issues remain outstanding?

#5 - 2008-07-07 08:04 - yagisan

Logged In: YES
user_id=1248824
Originator: NO

Changes From 1.9.0beta5.1 to 1.9.0beta5.2 and SVN trunk.

- Attempt to fix CVE-2007-4643 by discarding all runt packets. Luigi Auriemma’s exploit 3 fails against this patch. * Attempt to fix CVE-2007-4642 - Luigi Auriemma’s exploit 1 D_NetPlayerEvent global buffer-overflow using PKT_CHAT and exploit 2 Msg_Write global buffer-overflow through PKT_CHAT no longer effective. * Block off other possible msgBuff overflow vectors - no known exploits for these - yet * Attempt to fix CVE-2007-4642 - Luigi Auriemma’s exploit 4 static buffer-overflow in NetSv_ReadCommands no longer effective. * Attempt to fix CVE-2007-4642 - undelimited strcpy in PKT_CHAT - no known exploits of this.

See Commits:
r5032
Attempt to fix CVE-2007-4643 by discarding all runt packets. Luigi Auriemma's exploit 3 fails against this patch. This is an awful hack - we really need to replace the netcode

r5033
Attempt to fix CVE-2007-4642 - Luigi Auriemma's exploit 1 D_NetPlayerEvent global buffer-overflow using PKT_CHAT and exploit 2 Msg_Write global buffer-overflow through PKT_CHAT no longer effective. Fix works by clamping the copying to NETBUFFER_MAXMESSAGE chars at most

r5034
Block off other possible msgBuff overflow vectors - no known exploits for these - yet

r5035
Attempt to fix CVE-2007-4642 - Luigi Auriemma's exploit 4 static buffer-overflow in NetSv_ReadCommands no longer effective. Fix works by discarding all commands in excess of MAX_COMMANDS

r5036
Attempt to fix CVE-2007-4642 - undelimited strcpy in PKT_CHAT - know known exploits of this. Fix works by utilising a smarter string copy that is bounds checked to ensure all strings are null terminated - even if it means discarding input

CVE-2007-4644
I can trigger CVE-2007-4644, and it results in the clients crashing. It is a formatted strings bug. In theory it could use used to execute arbitrary code.

Please - run the exploit code against Doomsday - you'll easily see what is remaining. I emailed you about this last year - before I left the team. I think the right solution is to rip out all your netcode, and replace it with a sanity checked netcode. Do not blindly trust the clients.

#6 - 2011-12-15 15:41 - skyjake

Network messaging has been revised for 1.9.7.