

[NEWS] Doomsday Format String

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-04/msg00008.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 4 Apr 2006 11:06:17 +0200
-

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>
-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.
<http://www.securiteam.com/maillinglist.html>

Doomsday Format String

SUMMARY

The <<http://www.doomsdayhq.com/>> Doomsday engine is an enhanced and well known open source port of the original Doom engine and is also one of the most played on Internet.

Doomsday engine is vulnerable to a Format String vulnerability, allowing remote code execution on the server or connected clients.

DETAILS

The Doomsday engine contains many functions used for the visualization of the messages in the console. Both Con_Message and conPrintf are vulnerable to a format string vulnerability which could allow an attacker to execute malicious code versus the server or the clients. The first function calls a "Con_Printf(buffer)" while the second one calls a "SW_Printf(prbuff)" if SW_IsActive is enabled (which means ever).

Proof of concept:

Connect with telnet to port 13209 (default) of a DoomsDay server and type:

```
JOIN 1234 %n%n%n%n%n%n%n
```

The server will crash immediately.

[NEWS] Doomsday Format String

Vulnerable code (Src/con_main.c):

```
void Con_Message(const char *message, ...)
{
    va_list argptr;
    char *buffer;

    if(message[0])
    {
        buffer = malloc(0x10000);

        va_start(argptr, message);
        vsprintf(buffer, message, argptr);
        va_end(argptr);

#ifdef UNIX
        if(!isDedicated)
        {
            // These messages are supposed to be visible in
            // the real console.
            fprintf(stderr, "%s", buffer);
        }
#endif

        // These messages are always dumped. If consoleDump is
        // set,
        // Con_Printf() will dump the message for us.
        if(!consoleDump)
            printf("%s", buffer);

        // Also print in the console.
        Con_Printf(buffer);

        free(buffer);
    }
    Con_DrawStartupScreen(true);
}

..

void conPrintf(int flags, const char *format, va_list args)
{
    unsigned int i;
    int lbc; // line buffer cursor
    char *prbuff, *lbuf = malloc(maxLineLen + 1);
    cbline_t *line;

    if(flags & CBLF_RULER)
    {
        Con_AddRuler();
        flags &= ~CBLF_RULER;
    }
}
```

[NEWS] Doomsday Format String

```
}  
  
// Allocate a print buffer that will surely be enough (64Kb).  
// FIXME: No need to allocate on EVERY printf call!  
prbuff = malloc(65536);  
  
// Format the message to prbuff.  
vsprintf(prbuff, format, args);  
  
if(consoleDump)  
fprintf(outFile, "%s", prbuff);  
if(SW_IsActive())  
SW_Printf(prbuff);  
...  

```

Fix:
No fix, no reply from the developers.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:aluigi@xxxxxxxxxxxxxx>> Luigi Auriemma.

The original article can be found at:
<<http://aluigi.altervista.org/adv/doomsdayfs-adv.txt>>
<http://aluigi.altervista.org/adv/doomsdayfs-adv.txt>

=====

This bulletin is sent to members of the SecuriTeam mailing list.
To unsubscribe from the list, send mail with an empty subject line and body to:
list-unsubscribe@xxxxxxxxxxxxxx
In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxx

=====
=====

DISCLAIMER:
The information in this bulletin is provided "AS IS" without warranty of any kind.
In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.