

# [NT] Website Pro Path Disclosure (%20, ")

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-02/0105.html>

---

*From:* [support@securiteam.com](mailto:support@securiteam.com)

*Date:* 02/17/02

From: [support@securiteam.com](mailto:support@securiteam.com)

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

Date: Sun, 17 Feb 2002 11:31:31 +0100 (CET)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

-----

Website Pro Path Disclosure (%20, ")

---

## SUMMARY

<<http://website.deerfield.com/>> Website Pro by Deerfield was the first webserver developed for the Windows operating system and has a broad user base. A security vulnerability in the product allows remote attackers to cause the product to reveal its true path.

## DETAILS

Vulnerable systems:

Website Pro version 3.1 and prior

Certain malformed URLs result in the disclosure of the true path and location of the website html files:

<http://127.0.0.1/index.html>"

Or

<http://127.0.0.1/index.html%20>

Will cause the server to reveal the location of the web-root:

---

403 Forbidden

File for URL /index.html" (C:\www root\index.html") cannot be accessed:

```
<pre> The filename, directory name, or volume label syntax is incorrect.
(code=123)</pre>
```

---

Securiteam: [NT] Website Pro Path Disclosure (%20, ")

Impact:

The actual location of the files being served by the webserver is valuable intelligence for the malicious attacker.

Armed with such information, constructing code that may take advantage of flaws in scripting languages could be much simpler.

Workaround:

Ensure you are running the most recent version of Website Pro.

Vendor status:

Deerfield was notified 03/01/2002, although they acknowledged receipt of the email advising them of the vulnerability no further action has arisen.

ADDITIONAL INFORMATION

The information has been provided by <mailto:[labrat@interrorem.com](mailto:labrat@interrorem.com)> Russ Spooner.

=====

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](mailto:list-unsubscribe@securiteam.com)

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

- 
- **Previous message:** [support@securiteam.com](mailto:support@securiteam.com): "[NT] Phusion Webserver File Viewing, DoS and Arbitrary Code Execution Vulnerabilities"
  - **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)