

[NT] WinSCP Denial of Service

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-04/0053.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 04/15/04

To: list@securiteam.com

Date: 15 Apr 2004 19:39:40 +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>

WinSCP Denial of Service

SUMMARY

<<http://winscp.sourceforge.net>> WinSCP is "an open source SFTP (SSH File Transfer Protocol) and SCP (Secure CoPy) client for Windows using SSH (Secure SHell). Its main function is safe copying of files between a local and a remote computer". A malicious attacker can send an email containing a link that will cause WinSCP to crash.

DETAILS

Vulnerable Systems:

* WinSCP version 3.5.6 (prior versions might be also vulnerable)

The default installation of WinSCP provides the user with functionality to handle sftp:// and scp:// addresses. The vulnerability exists due to the way the application handles long URL's. A malformed scp:// or sftp:// address embedded in a HTML tag causes the WinSCP application to exhaust CPU and Memory resources. The attacker would need the ability to convince the user to visiting a web site he controlled or opening an HTML e-mail he had prepared. During the denial of service, WinSCP will not display any GUI.

Proof of Concept:

Securiteam: [NT] WinSCP Denial of Service

```
vibas.WriteLine("quote = Chr(34)");  
vibas.WriteLine("pgm = \"explorer\"");  
vibas.WriteLine("shell.Run quote & DoS & quote & \" \" & param");
```

```
vibas.Close();
```

```
</script>
```

```
</head>
```

```
</html>
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:luca.e@seeweb.it> Luca Ercoli.

=====

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.