

[NT] Ipswitch WhatsUp Gold prn.htm DoS

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-09/0044.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 09/19/04

To: list@securiteam.com

Date: 19 Sep 2004 14:29:33 +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 Gold prn.htm DoS

SUMMARY

Ipswitch WhatsUp Gold is a Microsoft Windows based network monitoring application. Remote exploitation of a denial of service vulnerability in Ipswitch Inc.'s WhatsUp Gold allows attackers to cause the application to crash.

DETAILS

Vulnerable Systems:

- * Ipswitch's WhatsUp Gold version 8.03
- * Ipswitch's WhatsUp Gold version 8.03 Hotfix 1

Immune Systems:

- * Ipswitch's WhatsUp Gold version 8.03 Hotfix 2

The problem specifically exists in the handling of reserved DOS device names. By generating a GET request for 'prn.htm' to the HTTP daemon installed by WhatsUp Gold, the application crashes and the following Runtime Library error is displayed:

Runtime Error!

Program: C:\Program Files\WhatsUp\whatsupg.exe

Securiteam: [NT] Ipswitch WhatsUp Gold prn.htm DoS

abnormal program termination

Analysis:

Successful exploitation allows unauthenticated remote attackers to crash the WhatsUp Gold application, thereby preventing legitimate usage. The WhatsUp Gold web server is not enabled by default.

Vendor response:

A patch to address this issue is available at:

<<http://www.ipswitch.com/Support/WhatsUp/patch-upgrades.html>>

<http://www.ipswitch.com/Support/WhatsUp/patch-upgrades.html>

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0799>>

CAN-2004-0799

Disclosure timeline:

08/12/2004 Initial vendor notification

08/12/2004 iDEFENSE clients notified

08/12/2004 Initial vendor response

09/16/2004 Coordinated public disclosure

ADDITIONAL INFORMATION

The information has been provided by <mailto:iDEFENSE>

idlabs-advisories@idefense.com.

The original article can be found at:

<<http://www.idefense.com/application/poi/display?id=142&type=vulnerabilities>>

<http://www.idefense.com/application/poi/display?id=142&type=vulnerabilities>

=====

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.