

[NT] DoS and Directory Traversal Vulnerabilities in WebServer 4 Everyone

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-10/0061.html>

From: support@securiteam.com

Date: 10/16/02

From: support@securiteam.com

To: list@securiteam.com

Date: 16 Oct 2002 02:56:50 +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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

DoS and Directory Traversal Vulnerabilities in WebServer 4 Everyone

SUMMARY

RadioBird Software's <<http://www.freeware.lt/>> WebServer 4 Everyone is a free "Powerful, MultiClient, yet Easy to handle and maintain, WebServer".

Two security vulnerabilities have been found in the product allowing remote attackers to cause the program to no longer process legitimate requests and to allow attackers to download files that reside the outside bounding HTML root directory.

DETAILS

Vulnerable systems:

- * WebServer 4 Everyone versions 1.23 and 1.27

Immune systems:

- * WebServer 4 Everyone version 1.30

Issue 1:

Improper bounds checking allow attackers to launch a denial of service (DoS) attack, causing the web server to crash. The condition is triggered when the software receives a request for a long filename, such as GET /AAAAAAAA...3000...AAAA HTTP/1.1 .

Securiteam: [NT] DoS and Directory Traversal Vulnerabilities in WebServer 4 Everyone

Issue 2:

A directory traversal issue exists. The software can be duped into serving a restricted file. This is done if an attacker issues a directory traversal request with the hexadecimal representation for the front slash character (%2F). For example, if the URL <http://target.server/%2f..%2f..%2f../winnt/repair/sam> were sent to a target server, the SAM table would be retrieved.

Analysis:

For Issue 1, exploitation could allow an attacker to deny legitimate users access to the server and the contents that it provides.

For Issue 2, exploitation allows an attacker to obtain sensitive information, such as the Windows NT SAM table. This kind of information can allow further compromise of the targeted host. Sensitive information such as credit cards can also be retrieved.

Customers should note that a remote user with access to the application can launch these attacks.

Vendor fix:

Leonardas Survila of Radiobird Software released WebServer 4 Everyone, version 1.30, which fixes the problems. It is downloadable at

<<ftp://ftp.freeware.lt/anonymous/Soft/w4asetup.exe>>

<ftp://ftp.freeware.lt/anonymous/Soft/w4asetup.exe>.

Disclosure timeline:

10/06/2002 Issues disclosed to iDEFENSE

10/14/2002 Vendor notified via e-mail to ulterior@freeware.lt

10/14/2002 iDEFENSE clients notified

10/14/2002 Response received from Leonardas Survila (leonardass@iki.lt)

10/15/2002 Vendor fix created

10/15/2002 Coordinated public disclosure

ADDITIONAL INFORMATION

The original advisory can be downloaded from:

<<http://www.idefense.com/advisory/10.15.02.txt>>

<http://www.idefense.com/advisory/10.15.02.txt>

The information has been provided by <<mailto:dendler@idefense.com>> David Endler of iDEFENSE and <<mailto:ts@securityoffice.net>> Tamer Sahin for finding the problem.

=====

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.

-
- ***Previous message:*** support@securiteam.com: "[\[NT\] Security Vulnerabilities in Polycom ViaVideo Web Component](#)"
 - ***Messages sorted by:*** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)