

[NT] MicroWorld eScan Server Directory Traversal

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2008-03/msg00017.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 10 Mar 2008 17:18:40 +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>

MicroWorld eScan Server Directory Traversal

SUMMARY

"The Powerful Management Console of <<http://www.mwti.net>> eScan provides options for system administrators to remotely administer a vast network of clients. It also allows them to remotely install eScan, deploy upgrades and updates and enforce an Integrated Security Policy for the entire Enterprise." A vulnerability in the way the MicroWorld eScan server works allows remote attackers to cause the product to provide access to files that would be otherwise inaccessible.

DETAILS

Vulnerable Systems:

* MicroWorld eScan Server (aka eScan Management Console) version 9.0.742.98

The eScan Server (eserv.exe) listens on port 2021 for FTP connections using c:\pub as root path.

Although the server tries to avoid possible directory traversal attacks for example rejecting the dotdot patterns, is still possible for an attacker to download any file from the disk of the remote system simply

[NT] MicroWorld eScan Server Directory Traversal

applying a slash or a backslash at the beginning of the filename for selecting the root path of the disk. For example /boot.ini, \windows\win.ini and so on.

Only downloading files is allowed by the server, so deleting or uploading custom files is not possible.

Exploit:

Clicking on the following URL:

<ftp://SERVER:2021//windows/win.ini>

Or manually:

```
ftp -A
open SERVER 2021
get
/windows/win.ini
local_win.ini
```

ADDITIONAL INFORMATION

The information has been provided by <<mailto:alugi@xxxxxxxxxxxxx>> Luigi Auriemma.

The original article can be found at:

<<http://alugi.altervista.org/adv/escaz-adv.txt>>

<http://alugi.altervista.org/adv/escaz-adv.txt>

=====

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@xxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxx

=====

=====

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.