

[NT] RaidenHTTPD Directory Traversal

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-02/0020.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 02/06/05

To: list@securiteam.com

Date: 6 Feb 2005 18:12:15 +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>

RaidenHTTPD Directory Traversal

SUMMARY

<<http://www.raidenhttpd.com/>> RaidenHTTPD is "a full featured web server software for Windows 98/Me/2000/XP/2003 platforms".

Due to improper testing by RaidenHTTPD of user provided filename, a remote attacker can cause the RaidenHTTPD to return the content of files that reside under the disk partition where the HTTPd has been installed.

DETAILS

Vulnerable Systems:

- * RaidenHTTPD version 1.1.27 and prior

Immune Systems:

- * RaidenHTTPD version 1.1.31 or newer

The program by default has some checks to avoid malicious patterns like "../" into HTTP requests, but the program doesn't well manage the initial "/" into requests. In fact if you send a request like:

```
GET /somefile HTTP/1.1
```

The web server will return the requested file if available in the

Securiteam: [NT] RaidenHTTPD Directory Traversal

DocumentRoot directory.

But if you send a request like:
GET somefile HTTP/1.1

The web server will return the requested file if available in the disk partition where the HTTPd is installed.

ADDITIONAL INFORMATION

The information has been provided by <mailto:fdonato@autistici.org>
Donato Ferrante.

=====

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.