

# [NT] Multiply Vulnerabilities in RaidenHTTPD

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-03/0004.html>

---

**From:** SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

**Date:** 03/07/05

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 7 Mar 2005 10:19:08 +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>

-----

## Multiply Vulnerabilities in RaidenHTTPD

---

### SUMMARY

" <<http://www.raidenhttpd.com/en/index.html>> RaidenHTTPD Server is a full featured web server software for Windows 98 / Me / 2000 / XP / 2003 platforms. It is easy to use and install, and is designed for anyone who wants to have a website running within minutes."

A buffer overflow vulnerability in Raiden HTTPD allows arbitrary code execution. In addition, a CGI source code disclosure vulnerability was found in RaidenHTTPD that may be exploited to obtain the source code of scripts on the server.

### DETAILS

#### Vulnerable Systems:

- \* RaidenHTTPD Server version 1.1.32

#### Immune Systems:

- \* RaidenHTTPD Server version 1.1.34

This document describes two vulnerabilities found in RaidenHTTPD server. The first vulnerability may be remotely exploited to obtain the source code of any PHP scripts on the server. The second is a buffer overflow

## Securiteam: [NT] Multiply Vulnerabilities in RaidenHTTPD

vulnerability that may be remotely exploited to cause DoS or to execute arbitrary code on the server.

### CGI source code disclosure vulnerability:

RaidenHTTPD supports the use of CGI scripts using PHP or PERL. The default installation comes with PHP installed. Using a specially crafted URL, it is possible to obtain the source code of any PHP scripts on the server.

### Buffer overflow vulnerability:

A buffer overflow condition occurs when RaidenHTTPD receives an URI with more than 524 characters in the URI. Successful exploitation allows code execution with LOCAL SYSTEM privilege.

### Disclosure Timeline:

- \* 02.20.05 – Vulnerability Discovered.
- \* 02.22.05 – Initial Vendor Notification.
- \* 02.22.05 – Initial Vendor Reply.
- \* 02.22.05 – Received notification from vendor that fixed version 1.1.34 is released.
- \* 03.01.05 – Public Release.

### Vendor Status:

Fixed version released(available for download <<http://www.raidenmaild.com/download/RaidenHTTPD.exe>> here).

### ADDITIONAL INFORMATION

The information has been provided by <<mailto:chewkeong@security.org.sg>>  
Chew Keong.

The original article can be found at:

<<http://www.security.org.sg/vuln/raidenhttpd1132.html>>  
<http://www.security.org.sg/vuln/raidenhttpd1132.html>

=====

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](mailto:list-unsubscribe@securiteam.com)

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@securiteam.com](mailto: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.