

# [UNIX] PHP Nuke Path Disclosure Vulnerability through Modules.php

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-03/0080.html>

---

*From:* [support@securiteam.com](mailto:support@securiteam.com)

*Date:* 03/18/02

From: [support@securiteam.com](mailto:support@securiteam.com)

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

Date: Mon, 18 Mar 2002 09:09:55 +0100 (CET)

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.

-----

PHP Nuke Path Disclosure Vulnerability through Modules.php

---

## SUMMARY

PHP Nuke exposes the real path where PHP scripts are located. This can give valuable information to attacker when planning the attack.

## DETAILS

For example:

<http://example.com/modules.php?op=modload>>

will return:

```
Warning: Failed opening 'modules/0/0.php' for inclusion
(include_path='.:usr/local/lib/php') in
/users/thisuser/example.com/modules.php on line 23
```

## ADDITIONAL INFORMATION

The information has been provided by <<mailto:patryk@newyork.com>> Patryk K. (echo7).

=====

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.

- 
- **Previous message:** [support@securiteam.com](mailto:support@securiteam.com): "[REVS] Fingerprinting Port 80 Attacks: A Look into Web Server, and Web Application Attack Signatures: Part Two"
  - **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)