

# [NEWS] H-Sphere CGI Information Disclosure Vulnerability

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2001-10/0018.html>

---

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

*Date:* 10/06/01

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

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

Subject: [NEWS] H-Sphere CGI Information Disclosure Vulnerability

Message-Id: <20011006204906.35043138C9@mail.der-keiler.de>

Date: Sat, 6 Oct 2001 22:49:06 +0200 (CEST)

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.

-----

H-Sphere CGI Information Disclosure Vulnerability

---

## SUMMARY

<<http://www.psoft.net/index.html>> H-Sphere is a scalable multi-server control panel for automating web-hosting tasks. A security vulnerability in the product allows attackers to view files that reside outside the normal bound HTML root directory.

## DETAILS

Vulnerable systems:

H-Sphere version 2.5 and prior

Immune systems:

H-Sphere version 2.6

H-Sphere does not filter out '../' character sequences from incoming requests. A remote attacker with a valid web account on the server can craft a special URL request and obtain files on the server located outside of the web root directory.

Securiteam: [NEWS] H-Sphere CGI Information Disclosure Vulnerab

Example:

http://[targethost]/some-path/psoft.hsphere.CP/some-path/?template\_name=../../../../../../../../etc/passwd

ADDITIONAL INFORMATION

The information has been provided by <mailto:[crazy\\_einstein@yahoo.com](mailto:crazy_einstein@yahoo.com)>  
Crazy Einstein.

=====

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): "[EXPL] A Security Vulnerability in AIM Causes a DoS (Exploit)"
  - **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)