

# [NT] Multiple Vulnerabilities in the Enceladus Server Suite (CSS, Clear text passwords, User file)

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-06/0045.html>

---

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

*Date:* 06/16/03

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

Date: 16 Jun 2003 11:52:21 +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

Latest attack techniques.

You're a pen tester, but is google.com still your R&D team?

Now you can get trustworthy commercial-grade exploits and the latest techniques from a world-class research group.

Learn more at <http://www.coresecurity.com/promos/site1>,  
or call 617-399-6980

-----

Multiple Vulnerabilities in the Enceladus Server Suite (CSS, Clear text passwords, User file)

---

## SUMMARY

<<http://www.mollensoft.com>> Enceladus Server Suite is "an Internet/Intranet lightweight Web and FTP Server for Windows, provides secure file sharing on any network! Perfect for Broadband, Cable Modem, Small business and Personal Use". Multiple vulnerabilities have been found in the product allowing remote attackers to insert malicious HTML or JavaScript into existing web pages, view the users' password without requiring any decryption, and to access the user database (containing usernames and passwords).

## DETAILS

Vulnerable systems:

\* Enceladus Server Suite version 3.9.11

Securiteam: [NT] Multiple Vulnerabilities in the Enceladus Server Suite (CSS, Clear text passwords, User file)

- 1) Enceladus Server Suite stores all usernames and passwords under the folder \Program Files\enceladus\users in clear text. Under the folder there is a file for each user (the file name is named after the username) and inside the file the password can be found (without any protection).
- 2) Any remote user can "Sign The GuestBook" with CSS (under the "E-mail Address" field or under the "Comments" Field ).
- 3) Any authorized user that has the security rights to download files from the "Secure File Downloads" can download the htaccess.txt file which contains all the usernames and their passwords to the "Secure Download" folder.

ADDITIONAL INFORMATION

The information has been provided by <mailto:vulncode@yahoo.com> Ziv Kamir.

=====

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.