

# [UNIX] YaBB Forum member.vars CRLF Injection Privilege Escalation Vulnerability

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-06/msg00020.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxx)>
  - *Date:* 13 Jun 2007 10:33:36 +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>

-----

YaBB Forum member.vars CRLF Injection Privilege Escalation Vulnerability

---

## SUMMARY

<<http://www.yabbforum.com/>> YaBB (Yet another Bulletin Board) is "an Open Source community forum system written in Perl". Remote exploitation of an input validation error within version 2.1 of YaBB Forum allows attackers to register with forum Administrator privileges.

## DETAILS

Vulnerable Systems:

- \* YaBB Forum version 2.1

The problem specifically exists due to insufficient validation when writing to the "vars" file for each user. By setting the values of certain variables to contain certain characters, attackers can elevate their privileges to that of the forum Administrator.

Analysis:

Exploitation allows attackers to obtain Administrator privileges, which include the ability to modify forum templates (i.e., Perl code). This allows administrators to execute arbitrary commands in the context of the

## [UNIX] YaBB Forum member.vars CRLF Injection Privilege Escalation Vulnerability

web server running the forum.

This attack can be performed during registration. This allows unauthenticated attackers to obtain forum Administrator privileges at registration time via the register.pl script.

Additionally, once registered, a forum user can modify their profile and conduct this attack using the profile.pl script.

Workaround:

Disabling the registration feature of the forum mitigates this issue.

Vendor response:

The YaBB Forum team has addressed this vulnerability by releasing a software update. For more information consult the following announce on their home site.

<http://www.yabbforum.com/community/?board=general:action=display:num=1181678785>  
<http://www.yabbforum.com/community/?board=general:action=display:num=1181678785>

Disclosure Timeline:

05/23/2007 – Initial vendor notification

05/23/2007 – Initial vendor response

06/12/2007 – Coordinated public disclosure

### ADDITIONAL INFORMATION

The information has been provided by

<mailto:idlabs-advisories@xxxxxxxxxxxxx> iDefense Labs Security Advisories.

The original article can be found at:

<http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=538>

<http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=538>

=====

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@xxxxxxxxxxxxx](mailto:list-unsubscribe@xxxxxxxxxxxxx)

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@xxxxxxxxxxxxx](mailto:list-subscribe@xxxxxxxxxxxxx)

=====

=====

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.