

[UNIX] phpScheduleIt Multiple Cross-Site Scripting And Privilege Escalation Vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-09/0019.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 09/08/04

To: list@securiteam.com

Date: 8 Sep 2004 09:06:56 +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>

phpScheduleIt Multiple Cross-Site Scripting And Privilege Escalation
Vulnerabilities

SUMMARY

<<http://www.php.brickhost.com/>> phpScheduleIt is a web application that attempts to solve the problem of scheduling and managing resource utilization. It provides a permissions-based calendar that allows users to self-register and reserve resources and the tools to manage those reservations.

phpScheduleIt is exposed to several XSS and privilege escalation attacks that allow any user to gain administrative rights.

DETAILS

Vulnerable Systems:

* phpScheduleIt version 1.0.0 RC 1

Cross-Site Scripting

When a new user is registering in the system, the "Name" and "Last Name" fields allow dangerous HTML tags and client side scripts to be inserted, due to improper sanitation. A simple way to test this vulnerability it to

Securiteam: [UNIX] phpScheduleIt Multiple Cross-Site Scripting And Privilege Escalation Vulnerabilities

register a new user and in one of the fields, entering the following:

```
<scr!pt>alert(document.cookie)</scr!pt>
```

On top of that, the system doesn't perform any kind of Email verification and thus a bot can easily render the system inoperable to all others by performing successive registrations, thus clouding the effectiveness of the entire system.

Likewise, when creating a new schedule, an attacker is able to insert potentially dangerous HTML and script code via the "Schedule Name" field, again improperly sanitized. This could lead to the exact same impact as the previous XSS described and can be tested in exactly the same manner.

Finally, a privilege escalation vulnerability exists which allows a normal unprivileged users on the same machine to gain administrative privileges when the real administrator does not perform a logout from the system. This issue exists due to sessions cookies incorrectly handled and/or not deleted.

Vendor Status:

The vendor is aware of the bugs and has fixed them. The fixed version will be available in the upcoming release.

ADDITIONAL INFORMATION

The information has been provided by <mailto:joxeankoret@yahoo.es> Joxean Koret.

=====

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.