

[UNIX] phpAdsNew and phpPgAds Multiple Vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-03/msg00087.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxx>
 - *Date:* 27 Mar 2006 19:06:41 +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>

phpAdsNew and phpPgAds Multiple Vulnerabilities

SUMMARY

<<http://phpadsnew.com/two/>> phpAdsNew is "an open-source ad server, with an integrated banner management interface and tracking system for gathering statistics." <<http://phpadsnew.com/two/>> phpPgAds is "a port of phpAdsNew that uses PostgreSQL as its database backend, instead of MySQL." Both phpAdsNew and phpPgAds products have been found to contain HTML/JavaScript injection vulnerabilities.

DETAILS

Vulnerable Systems:

- * phpAdsNew version 2.0.7
- * phpPgAds version 2.0.7

Immune Systems:

- * phpAdsNew version 2.0.8
- * phpPgAds version 2.0.8

HTML injection / Cross-site scripting in the admin interface
Some scripts inside the admin interface were displaying parameters

[UNIX] phpAdsNew and phpPgAds Multiple Vulnerabilities

collected by the delivery scripts without proper sanitizing or escaping. The delivery scripts have public access, while the admin interface is restricted to logged in users. An attacker could inject HTML/XSS code which could be displayed/executed in a later time inside the admin interface.

Solution:

Upgrade to phpAdsNew or phpPgAds version 2.0.8.

HTML injection / Cross-site scripting in the login form

The login form was sending back to the browser the unmodified query string, making possible for an attacker to inject HTML/XSS code by using a specifically crafted URL.

Solution:

Upgrade to phpAdsNew or phpPgAds version 2.0.8.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:matteo@xxxxxxxxxxxx>> Matteo Beccati.

=====

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@xxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxx

=====
=====

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.