

# [UNIX] WHM AutoPilot Privileges Escalation

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-11/0075.html>

---

**From:** SecuriTeam (*support\_at\_securiteam.com*)

**Date:** 11/21/05

To: list@securiteam.com

Date: 21 Nov 2005 16:23:49 +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>

-----

WHM AutoPilot Privileges Escalation

---

## SUMMARY

" <<http://www.whmautopilot.com/>> WHM AutoPilot is a web hosting management tool."

WHM AutoPilot does not validate user account rights, allowing any user to cancel any web hosting account, regardless of the web account owner.

## DETAILS

Vulnerable Systems:

\* WHM AutoPilot version 2.5.20 and prior

A vulnerability leading to unauthorized cancellation requests has been found.

The "c" GET variable sent to /cancel\_account.php is not verified to ensure that the currently logged in user owns the account specified by the base 64 encoded integer value (the ID of the hosting account one wishes to cancel).

An attacker with an account in a WHMAP installation could file cancellation requests for hosting accounts that do not belong to the

Securiteam: [UNIX] WHM AutoPilot Privileges Escalation

attacker's account.

In the worst case these cancellation requests would be processed by the authority running WHMAP, and the targeted hosting accounts would be canceled.

Workaround:

There is no known workaround at this time.

Disclosure Timeline:

Discovered: November 16, 2005

Vendor Notified: November 17, 2005

Public Release: November 17, 2005

ADDITIONAL INFORMATION

The information has been provided by <mailto:agna\_zilchi@linuxmail.org>  
Agna Zilchi.

=====

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.