

[UNIX] Alstrasoft Epay Pro Directory Traversal

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-09/0117.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 09/29/05

To: list@securiteam.com

Date: 29 Sep 2005 15:38:11 +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>

Alstrasoft Epay Pro Directory Traversal

SUMMARY

<<http://www.alstrasoft.com/epay.htm>> EPay Pro is "the ultimate software solution for those who wish to run their own Paypal, Stormpay, or e-gold type of online business. Epay Pro comes with a ready out of the box website with all the features you need to run your own payment gateway system".

Alstrasoft Epay Pro has been found to be vulnerable to a directory traversal vulnerability, allowing remote attackers to access sensitive information on the vulnerable system.

DETAILS

Vulnerable Systems:

* Epay Pro versions 2.0 and prior

Epay's Pro vulnerability caused by an improper validation of user-supplied input.

A remote attacker could embed in the index.php etc/passwd containing embedded code in the payment or send parameter which, once the link is clicked, would be executed to see passwords within the security context of

Securiteam: [UNIX] Altrasoft Epay Pro Directory Traversal

the hosting server. An attacker could use this vulnerability to see all the victim's password authentication credentials.

Example:

<http://targeturl/index.php?read=../../../../../../../../../../../../etc/passwd>

ADDITIONAL INFORMATION

The information has been provided by <mailto:GeMeGeMeS@Gmail.Com> GeMeGeMeS.

The original article can be found at:

<<http://h4cky0u.org/advisories/HYA-2005-008-altrasoft-epay-pro.txt>>

<http://h4cky0u.org/advisories/HYA-2005-008-altrasoft-epay-pro.txt>

=====

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.