

## Aggiornamento della sicurezza (#2)

(22/03/2006) In rete si sono diffuse alcune tecniche di spamming denominate "form-hijacking" che, al fine di spedire messaggi e-mail in modo anonimo, inviano dati appositamente predisposti a script lato server individuati più o meno a caso. Tali dati "simulano" gli header di un messaggio e-mail.

Un attacco di questo tipo, rivolto ad un negozio realizzato con eDisplay ENTERPRISE, produce ordini "strani" contenenti un indirizzo e-mail ripetuto più volte, e corrispondenti e-mail di notifica inviate all' esercente. Questo meccanismo non è pericoloso in sé (non c'è un tentativo di "hackerare" il server o impossessarsi dei dati) ma va comunque impedito.

- Per i negozi che utilizzano uno script *edorder.php* standard, la soluzione consiste nell'utilizzare lo script *edorder.php* aggiornato scaricabile qui:

[http://www.edisplay.it/enterprise/download/security\\_sr2.zip](http://www.edisplay.it/enterprise/download/security_sr2.zip)

Sostituire, nella sottocartella *code*, questo script all'originale, quindi ricostruire ed aggiornare.

- Per i negozi che utilizzano uno script *edorder.php* modificato, la soluzione consiste nell'eseguire le modifiche al file *edorder.php* (si trova nella sottocartella *code*) descritte di seguito:

- Localizzare la riga:

```
$cliente = GetCliente();
```

ed aggiungervi subito di seguito le seguenti linee di codice:

```
if (($regobbl != 0 && $cliente == 0) ||  
    strpos($HTTP_POST_VARS['Totale_No_Spedizione'],'@') > 0 ||  
    strpos($HTTP_POST_VARS['Totale_Ordine'],'@') > 0 ||  
    $HTTP_POST_VARS['Process'] == '') die('.');
```

*L'aggiornamento deve essere eseguito da tutti gli utenti che dispongano di una qualsiasi edizione (include le versioni Small Business, Demo, Light e Client) con release 1.0.8 o inferiore; in caso di dubbio è comunque sempre possibile eseguire l'aggiornamento senza nessuna controindicazione.*