

[Full-disclosure] Cambiumgroup customers get hacked fast!

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2009-02/msg00143.html>

- *From:* angrycustomer@xxxxxxxxxxxxx
 - *Date:* Wed, 11 Feb 2009 15:44:19 -0500
-

Thought this might be the place to send this. We were using the content system that cambiumgroup created and it resulted in me losing my job because my employer got hacked. When I googled them I found this posting in google's cache.

<http://74.125.47.132/search?q=cache:PtwMBLcvxxsJ:www.vermontinternetdesign.com/index.php%3Ftopic%3D597.0+cambiumgroup+Vulnerabilities&hl=en&ct=clnk&cd=3&gl=us&client=safari>

Hello everyone I would like to share this post with everyone here on my site. I would like to talk about the safety of your email accounts and what is being done to protect them. Why its important that the owner of a web development company understands what they are doing.

Well email accounts are proly the most vulnerable part of any web server. Simply because email accounts are typically the most benifical to someone who is trying to breach your webserver. It is profitable for a hacker to breach an email account. Why? Well why is it profitable for you to do an email blast. The same reason it is for a hacker to do one.

I was working for a company in St. Johnsbury Vermont (Cambium Group LLC) for a couple of months. I was hired to do a backlog of projects that the lead developer obviously wasnt capable of doing. While I was working at this place I had noticed that someone had unauthorized access to the companies internal webservers. I mentioned to the owner of the company that someone had unauthorized access to the web server.

He thought that I was crazy that someone could have possibly done that. I simply couldnt sleep at night. I checked the webserver and found they were using a website monitoring service that had been hacked into. Meaning there was a program that they used that access all of the client webservers from there development server. Upon talking to the owner and Secretary of this company. I learned that either one of the owner of Cambium group or the Sales lady would admit

[Full-disclosure] Cambiumgroup customers get hacked fast!

that there was a problem. They were too worried about protecting a reputation than securing a web server.

After this incident I decided to do a further investigation. Upon closing my investigation I learned that the people that I was working for were selling a very unsecured content management system to Credit Unions. They had told me they wanted me to protect their clients accounts and websites. However when I mentioned that there were a lot of security holes they didn't want to take action to protect their customers. They simply did not care. I would like to make everyone aware of all of the problems that I found when working with <http://www.cambiumgroup.com> .

- 1) I found that all of their webservers use the same configuration. Big no no when you are working with banks.
- 2) I found that large volumes of spam was being sent from company and customer email accounts. Many customers were complaining that emails were being sent that they never sent.
- 3) I found that adding malformed urls to their content management system will allow a remote user to run mysql queries directly on their database.
- 4) I found that the admin password is the same on 100 websites
- 5) I found that the content management system would be vulnerable to both html injection and sql injection.
- 6) I found that their lead developer Jason Leno only knows basic programming skills and denies that someone would be able to cause a problem due to the above issues.
- 7) I found that the web forms they were using on their Content Management system would allow someone to send an email to a mailing list.
- 8) I found that Scott Wells and Shari Choinard had no interest in protecting their customers from the above issues.
- 9) I found out that they were charging \$20,000 – \$50,000 for an application that opens up the clients to the above vulnerabilities.
- 10) After working at this company for 2 months I learned that the secretary Shari, and Scott Wells live together and neither one of them knows anything about computer programming.

[Full-disclosure] Cambiumgroup customers get hacked fast!

[Full-disclosure] Cambiumgroup customers get hacked fast!

I am putting this posting here so to protect the customers of that company. I know there are paying alot of money for what they got and for the amount of money they are charged they should not be opened up to these security problems.

--

Be a professional. Click here to earn a psychology degree.

<http://tagline.hushmail.com/fc/PnY6qxultlrtwxI8C5TG1niHYrBtAWdFS2UrVp0KDdMdGEikS5kUY/>

Full-Disclosure – We believe in it.

Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>

Hosted and sponsored by Secunia – <http://secunia.com/>