

By: Fedor Grigores, SEO News Editor

[Firefox 2.0.0.11 and Opera 9.50 Information Leak!](#)

BMPs to blame

There's nothing to kick your morning into gear like finding out that your browser can be the means of losing personal information. I'm talking about the people who actually care and did not go with the stock Windows Internet Explorer, known to be flawed and continually exploited. Choosing the safer version for surfing the web, like Mozilla's Firefox or Opera, might prove, until this is fixed, to be a pretty big error. The problem is concerning the way the two browsers mentioned above handle a .BMP file, as Gynvael Coldwind posted on Vexillum.org. Breaking it down to the basics, a simple scanner/ harvester site, created by the cyber criminal, can copy the leaked data from Firefox and Opera memory onto a remote server. It does not select and sort what it copies, but rather takes it all in a bundle, but as it sometimes happens, some personal important information is available on your screen. Picture your Internet banking account being copied as a whole. The longer you stay on a site, the more data is leaked to the third, remote site. Depending on the capacity of the scanner and the rate it has been set to refresh, it will gather a set amount of information per each refresh. Coldwind demonstrated it with heaps of 7650 bytes and using a visible scanner, but if placed in a hidden iframe, it's almost impossible to find it. The vulnerability is caused by the BITMAPINFOHEADER field contained in the BMP format named biClrUsed, indicating how many colors the palette has. 0 = 256, any other number is its equivalent. According to Gynvael, both Firefox and Opera allocate to just the 'right' amount of memory or forget to nil the allocated palette. Translated into English, if there's nothing there, it will be a BMP that copies exactly what the screen displays at the moment. "If the attacker creates a BMP file with biClrUser = 0, and fills it with gradient, from 0 to 255: 00 01 02 03 04 05 ... and so on, the displayed BMP will in fact copy the palette to the screen, which ofcourse means that it copies the data lying on the heap to the screen," Coldwind says.. My advice would be to roll back to the versions you upgraded to this from, that seems to solve the problem.