

RE: [Full-disclosure] How many vendors knowingly ship GA product with security vulnerabilities?

RE: [Full-disclosure] How many vendors knowingly ship GA product with security vulnerabilities?

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2006-05/msg00083.html>

- *From:* "Bill Stout" <bill.stout@xxxxxxxxxxxxxxxxx>
 - *Date:* Thu, 4 May 2006 18:15:18 -0700
-

Thanks Vladis,

That's an excellent and well thought out reply. Sounds like you have some experience in delivering software.

It would seem that if a few days buffer were built into the system, specifically to check in security fixes prior to QA; that would be a huge 'CYA' benefit to prevent those 'CLM' moves and to protect the consumers of the software.

Bill Stout

-----Original Message-----

From: Valdis.Kletnieks@xxxxxx [<mailto:Valdis.Kletnieks@xxxxxx>]

Sent: Wednesday, May 03, 2006 11:10 PM

To: Bill Stout

Cc: full-disclosure@xxxxxxxxxxxxxxxxx

Subject: Re: [Full-disclosure] How many vendors knowingly ship GA product with security vulnerabilities?

On Wed, 03 May 2006 22:23:42 PDT, Bill Stout said:

If a patch is ready in just a few days, and QA for a patch takes several weeks, it would seem the vendor already knew about the vulnerability and had a fix ready, either for next release or vulnerability discovery,

It would *seem* that way, yes. But it often doesn't work that way.

RE: [Full-disclosure] How many vendors knowingly ship GA product with security vulnerabilities? 1

RE: [Full-disclosure] How many vendors knowingly ship GA product with security vulnerabilities?

Quite often, the bug is a Homer Simpson "D'Oh!" error (such as most buffer overruns), so a "first cut" of a patch can be done in a few *hours*.

which ever came first. Otherwise the fix would take weeks to test and release in order to test all compatibilities related to the bug fix, correct?

But it can *still* take a while to actually integrate and test the fix, especially if it involves an API change. For instance, a buffer overflow may be fixed by passing in a new "length" parameter. Then you have to find and fix all the places that call the function, to also pass the length, and then find all the places that call those places, and so far...

And if you're *really* unlucky, the API change goes to multiple code repositories for multiple products... and things get *really* ugly.

Try it sometime – pull down the source for Firefox or OpenOffice, which are "average" sized for large software systems. Unpack it someplace (make sure you have multiple gigabytes of disk available). Now find some random foo.h file somewhere in the tree. Find a 'struct' in that .h, and add one more thing to that struct. 'int blat;' is good enough. Now see how long it takes you to find every use of that struct, and add a 'foo_struct.blatt = 5;' (or 6, or 9, or different value at each use).

Then have fun tracking down all the *implicit* uses – code that uses sizeof(), or places where the code blows up if 'sizeof(struct foo_struct)' is over the size you can store in a certain field in a database. Oh, and don't forget to find that XML file that generates the marshal/demarshal code for this.... ;)

So, my question is, if the vendor knew about vulnerabilities before a product was released, why wouldn't they simply delay the ship a few days

in order to QA the patch for vulnerabilities they already knew about?

RE: [Full-disclosure] How many vendors knowingly ship GA product with security vulnerabilities? 2

RE: [Full-disclosure] How many vendors knowingly ship GA product with security vulnerabilities?

There's this thing called a 'freeze date', and it's often several
months
before the planned 'ship date'. You have to freeze the code at *some*
point,
do the QA, and at some point produce a .ISO or similar to send to burn
CDs.
Then you have to send the CD off to be duplicated (even a *big*
duplicating
shop is going to take a while to produce 10,000,000 burned, custom
artwork,
manuals, into a box and shrink wrapped and sent to Office Max and Best
Buy
and Walmart and everywhere else. Oh, and you need to send copies to
whatever
PC manufacturers bundle it, so Dell and HP and Levono can integrate it
into
the images *they* install.

So you're sitting there, 3 million CD's burned, Dell and HP ramping up
and
Levono ready to go tomorrow – and you want to *delay a few days* because
there might be a bug????

Somebody's gonna *pay* for that fuck-up. It's a CLM (Career-Limiting
Move).

<http://today.reuters.com/business/newsArticle.aspx?type=technology&storyID=nN02271704>

Vista is slipping *again*. And the news took MSFT stock down 0.22 to
\$24.07.
That's a 1% hit in market value. And that means that Gates's \$40B in
MSFT stock
just dropped \$400M in value. That means Gates is gonna rip Ballmer a
new one
(wouldn't *you* if you just lost \$400M?). Ballmer is gonna rip somebody
a new
one, and so on down the line.

You wanna be the software engineer at the end of that line? You're
gonna get
ripped so many new ones, you're gonna be called "Swiss Cheese" at your
next job...

And it's not limited to proprietary software either – the guys over at
Firefox just released 1.5.0.3 to fix a nasty flaw. Now, *somebody* had
to make
the hard call "We ship 1.5.0.3 *now* to fix this bug, and the stuff that
was
targeted for 0.3 is going to slip to 0.4". Do you want to be the

RE: [Full-disclosure] How many vendors knowingly ship GA product with security vulnerabilities? 3

RE: [Full-disclosure] How many vendors knowingly ship GA product with security vulnerabilities?

software

engineer that tries to say "Umm.. can we hold 0.3 for a week and a half
while

we get these 3 minor bugfixes finished?"

Full-Disclosure – We believe in it.

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

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