Rational Survivability

Hoff's Ramblings about Information Survivability, Information Centricity, Risk Management and Disruptive Innovation. Oh, I have a fondness for virtualization, too...
...It used to be titled 'Rational Security' but Security's DEAD, didn't ya know? ;->

July 23, 2008

The DNS Debacle In Poetic Review

A few months ago
Kaminsky discovered a flaw.
It was with DNS,
It was nasty and raw

> He decided than rather
> to disclose all at once
> he'd instead only tell people
> who'd fix it in months
>
> > So some meetings were had
> > and work soon began
> > vendors wrote patches
> > coordinated by Dan
> >
> > > Fast forward some time
> > > out the closet it came
> > > some researcher types
> > > got into the game
> > >
> > > > Dan's rules were quite simple,
> > > > that in 30 days
> > > > he'd present during Blackhat
> > > > and we'll all be amazed
> > > >
> > > > > A bunch of big egos
> > > > > called Dan on a bluff
> > > > > said his vuln was a copy
> > > > > of 10 year old stuff
> > > > >
> > > > > So Dan swore them on handshakes
> > > > > and details were provided
> > > > > and those same cocky claims
> > > > > soon all but subsided
> > > >
> > > > It seems that Dan's warnings
> > > > weren't baseless at all
> > > > Said the same skeptical hackers
> > > > "the risk isn't that small!"
> > >
> > > So Blackhat was nearing
> > > the web didn't break
> > > then out came a theory
> > > from our friend Halvar Flake
> >
> > No sooner had he posted
> > and described the vuln's guts
> > than Matasano's blog surfaced,
> > kicked the web in the nuts
>
> It said "Halvar's right!"
> we'll no longer keep quiet.
> The post's ripple effect
> caused a nasty 'net riot

The blog quickly was pulled
but the cat's out of the bag
the arms race began
since there's no longer a gag

> Meanwhile the issues of honor and trust
> rehashed the debate
> of when disclosure goes bust
>
> > So Dan's days of thirty
> > we never did see

> > thirteen is OK
> > but I issue this plea
> >
> > > When researchers consider
> > > how to disclose and thus when
> > > will you think of the users?
> > > How it might affect them?
> > >
> > > > This ego-fueled rush
> > > > to put your name on a vuln
> > > > has a much bigger impact
> > > > than you might have known
> > > >
> > > > > If the point here is really
> > > > > to secure and protect
> > > > > then consider what image
> > > > > you really project
> > > >
> > > > In this case the vuln.
> > > > is now in the wild
> > > > an exploit is coming
> > > > DNS soon defiled
> > >
> > > The arms race has started
> > > and the clock now is ticking
> > > If you haven't yet patched
> > > you'll soon take a licking
> >
> > I'm not taking sides really
> > on the disclosure debate
> > but rather the topic
> > of patch early or late
>
> What good is disclosure
> if the world couldn't cope
> with the resultant attacks
> if we've all got just hope?

There's two sides to this issue
both deserve merit
but Dan's rep has been smeared
I say let's just clear it

--

Happy patching everyone! ;(

/Hoff

12:31 AM in Poetry | Permalink
Technorati Tags: Chris Hoff, Christofer Hoff, Dan Kaminsky, DNS, Full Disclosure, Halvar Flake, Matasano, Rational Security, Rational Survivability

TrackBack

TrackBack URL for this entry:
http://www.typepad.com/t/trackback/866734/31529714
Listed below are links to weblogs that reference The DNS Debacle In Poetic Review:

Comments

Very nice. Now all we need is illustrations to put it into "Little Golden Book" children's book format :)

Posted by: Wesley McGrew | July 23, 2008 at 12:41 AM
Genius! Would've sent that compliment via Twitter but... fail whale.

Posted by: Chris Eng | July 23, 2008 at 01:20 AM
LOL. That's good one ;)

Posted by: Andrzej Dyjak | July 23, 2008 at 07:26 AM
Well said :)

Posted by: Andrew Hay | July 23, 2008 at 10:45 AM
I nominate you for a new Pwnie Award... best Security related poem.

-Nate

Posted by: Nate McFeters | July 23, 2008 at 11:23 AM
Bravo! How do we commission a "Twas the Night Before Black Hat" version? :)

Posted by: Crystal | July 23, 2008 at 09:26 PM
@Crystal...

Easy:

1) Rocks glass
2) 2 Ice cubes
3) 23yr old Pappy Van Winkle

...the beauty is, I happen to have all three. ;)

Posted by: Christofer Hoff | July 24, 2008 at 02:24 AM
Hoff, you deserve a t-shirt for this:
http://www.bustedtees.com/hassle

Posted by: Rani | July 24, 2008 at 03:51 AM
Obviously pissed at the entire circus with the DNS...
I must admit that the entire sharade reminded me of a circus between Zibri and George Hotz with the unlock of iPhone 1.2 OS - both were secretive and hiding the solution for a month to prove a better hero at the end.

Spirovski Bozidar
http://www.shortinfosec.net

Posted by: Bozidar Spirovski | July 24, 2008 at 12:13 PM