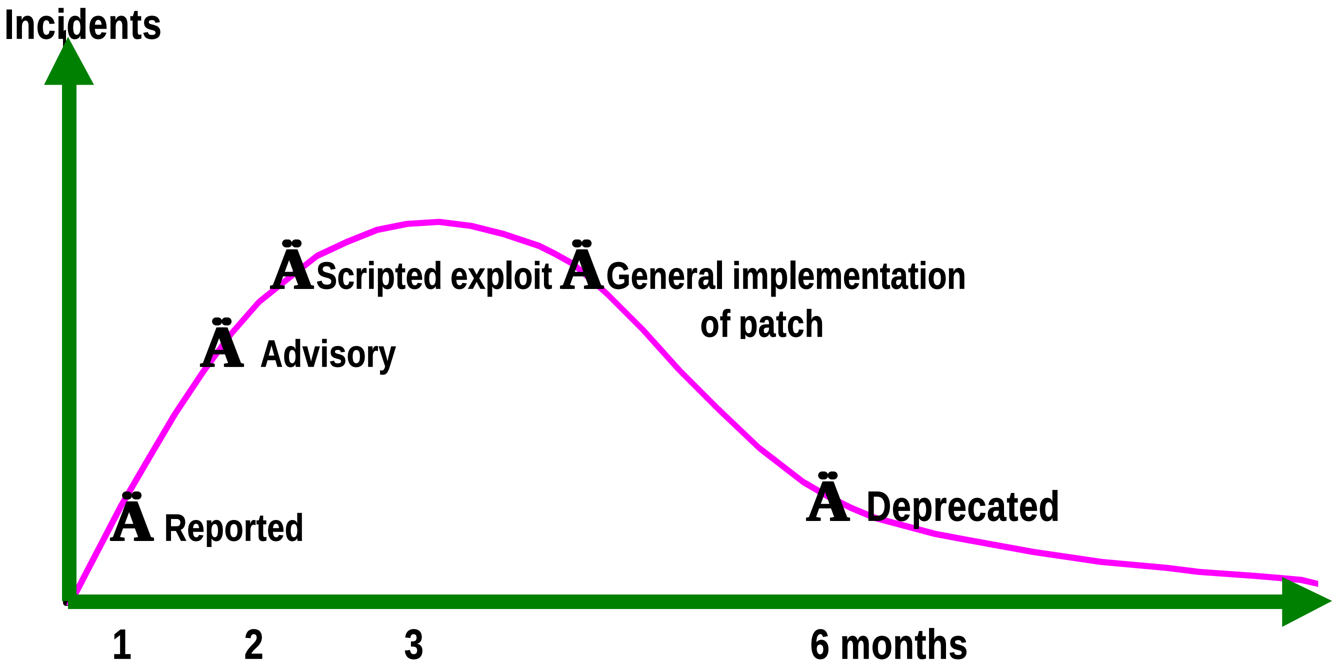
Osborne’s Vulnerability Lifetime Theory



1 Introduction

This little theory was first devised in late 2001 and presented at the E-security conference Oct 24, 2002. It is an attempt to explain the lifecycle stages of a vulnerability, which are:-

- Reported
- Advisory
- Scripted exploit
- Patch generally implemented
- Deprecated

It is based on hypothesis and observation NOT extensive statistical analysis.

vww.loud-fat-bloke.co.uk

2 Lifecycle stages

2.1 Reported

Until this point, you, as the discoverer, are getting your facts right. But you don't work alone and you share with your mates, so there may be uncodified incidents reported that will be later be attributed to this vulnerability.

2.2 Advisory

Once reported, Unix-lore requires that you give the vendor 30 days or until the patch is released, before you independently publish the vulnerability.

2.3 Scripted exploit

As soon as details of the vulnerability are published, someone will produce a scripted version of the exploit. This will result in a massive increase in the number of the attacks launched. Fortunately, this scripted exploit is released around the same time that the patch or fix is available (Why? – Sometimes the advisory fuels the production of the script – in other cases with less vigilant manufacturers the scripted exploit forces/encourages the manufacturer to produce the fix). Because of this, typically the implementation of the patch flattens the curve.

2.4 Patch generally implemented

For many large organisations, there is a huge logistical exercise involved in applying a patch to all productions servers. Many security "experts" forget that:

- Patches have to be tested – not only is it common-place for patches simply not to work. It is also common for patches to cause other OEM software to mal-function or to cause other vulnerabilities to emerge.
- Many organisations are enormous, and updating a core operating system on every platform will take a significant elapse time.

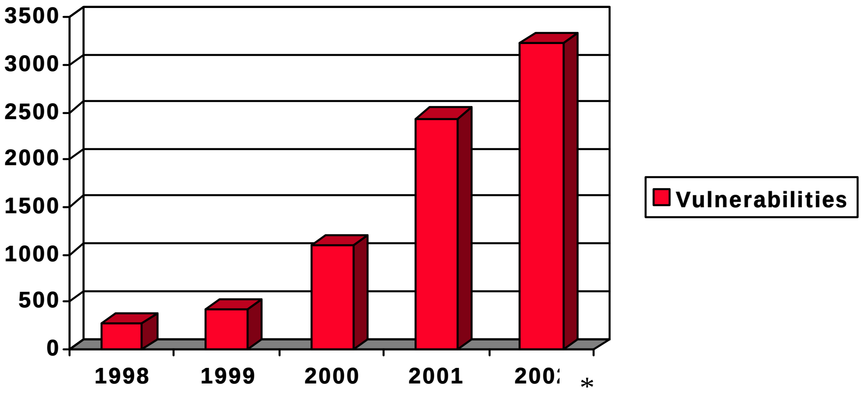
By this stage most (greater than 50%) of servers are patched, so the number of successful exploits will start to dip.

2.5 Deprecated

The vulnerability never really goes away because it gets embedded in commercial scanners. Alternatively, servers infected with *Nimda* or *Code-red* etc will still attack people run old vulnerable operating systems.

3 Why have I bothered

Unfortunately, much of the security community remain untouched by the reality of real-world computing. Currently, the burden of patch management is overloading most system administrators and change control systems.



** Figure for 3 of 4 quarters of 2002 Source Cert/cc*

With new security vulnerabilities being discovered at about 30/month, a better understanding of vulnerabilities can only lead to better patch management systems.