The Heartbleed bug continues to pose risks for people

July 4 2014, by Robert Merkel

The 4.1.1 version of Android's Jelly Bean operating system remains a risk. Credit: Flickr/Frikjan, CC BY-NC-ND

It's been almost three months since the Heartbleed bug was revealed and many thousands of computer servers still need to be fixed.

The Australian government's Stay Smart Online initiative this week points to research by security expert Robert Graham who identified

600,000 vulnerable servers after the Heartbleed bug was made public in April. He says 300,000 servers still remain exposed as of late June.

Managing security problems in complex IT infrastructure is uncannily like managing pests on a farm. If they are handled promptly, problems are minimised.

But if they are neglected, the problems will grow, do more damage and take more work to rectify when they are finally dealt with.

The equivalent of an insect plague arrived on the paddocks of the world's IT system administrators in April 2014 when the Heartbleed vulnerability was first revealed.

The Heartbleed risk

The Heartbleed bug was a programming mistake in the OpenSSL security library used by a large proportion of the world's internet software. It left much of the world's IT infrastructure vulnerable to cybercriminals.

Keeping systems secure required system administrators to not only update software, but obtain new "master keys" to re-establish their corporate electronic identity. In many cases they also had to ask their users to change passwords.

It is likely that the global cost of dealing with Heartbleed has already run into the hundreds of millions of dollars.

A second round of problems in the same software were identified in June 2014, again requiring considerable remedial action by vendors and system administrators.

But the problem persists

A few months on from Heartbleed the majority of internet-accessible systems that were vulnerable have been secured, but not all.

For instance, many older Android smartphones have a firmware version (4.1.1) that contained the vulnerable code. Protecting these phones required the firmware supplier to either patch the supplied version to fix the bug, or update to a newer version of Android.

While exploiting the bug on a smartphone is much harder than on a server, it remains possible. Therefore vulnerable phones should be updated to protect them.

Google made updates available to the manufacturers of smartphones shortly after discovering the problem but manufacturers then had to apply Google's fixes to the specific firmware for each of their affected models, and test the fixed version.

Even then, updates for many phones were not made available to consumers, as phones are often sold with customised firmware from carriers.

The major Australian carriers – Telstra, Optus and Vodafone – provide custom firmware in phones sold from their retail outlets. Each carrier would then have had to package and test the update for the customised version for each vulnerable phone model.

Given the relatively limited resources at each individual carrier for such testing, it's no surprise that this process took a long time. For instance, it took Vodafone Australia until June 16 to supply fixed firmware for one model, the HTC One X.

Other carriers, and other phones running this Android version, may still be vulnerable. Users of Android phones should consider downloading the free Lookout Heartbleed Detector from the Google Play store to check.

Why so slow to fix the bug?

The issues illustrated by the slow rollout of Android updates are specific examples of the kinds of problems faced by both software vendors and system administrators in dealing with security vulnerabilities.

Fixing the problem in the software is often the easy part. Deploying the fix across the many affected systems, and testing to ensure that the fix doesn't create additional problems, is where the real work lies, particularly when security updates are bundled with other unrelated fixes that may have side effects.

Information security analyst Marco Ostini, who works at the Australian Computer Emergency Response Team (AusCERT), says this leads to "vulnerability mitigation fatigue" where fixes are not being deployed on many systems.

The problem with orphans

The systems and software packages that aren't being updated are "orphans" – that is, no one is taking responsibility for keeping them updated to protect against security issues.

Phones running the vulnerable version of Android, 4.1.1, were actually examples of orphan devices, as most suppliers had ceased providing updates for them. Because of the scale of the security risk, an exception was made for Heartbleed.

IT orphan servers are often be operated by smaller organisations, or smaller divisions within larger ones, that lack the expertise to maintain their servers.

They may be running old, unsupported software that nevertheless continues to perform some useful but often relatively small task. A common example is a computer in an engineering environment such as a factory that uses vendor-specific software to control some expensive, valuable, but ageing device.

If the vendor has ceased to support the software, there may be no way to fix it. Even if the software is open source the individual customer will often not have the expertise to perform the fix themselves.

But sometimes orphan servers *are* simply the result of tired system administrators with the so-called "vulnerability mitigation fatigue". Maintaining servers, particularly running old and relatively unusual software, is a great deal of work and the rewards are often not clear.

If it ain't broke … still fix it

It's tempting to simply say "if it ain't broke, don't fix it". Unfortunately, IT security doesn't work that way.

Aside from the risk of data loss from the specific system, a compromised server within a wider corporate network may leave a gap in the metaphorical fence for further attacks.

Therefore, managing IT infrastructure requires vigilance to ensure even lower-profile systems are kept protected, and careful design to reduce the consequences of a single system being compromised.

Even if the consequences to the organisation of a compromise of a

particular system are not great, they still represent a safe and anonymous electronic haven from which cybercriminals can do further damage. In the farm analogy, they're the equivalent of the neglectful neighbour's weed-infested paddock.

The internet has become an essential part of our global society but it is vulnerable to criminal activity, and will ever be thus. The continuing aftermath of Heartbleed increases that vulnerability.

That is why we need diligence on the part of those who develop and manage IT systems to not only protect their own little patches, but to help keep the pests under control more generally.

This story is published courtesy of The Conversation *(under Creative Commons-Attribution/No derivatives).*

Source: The Conversation