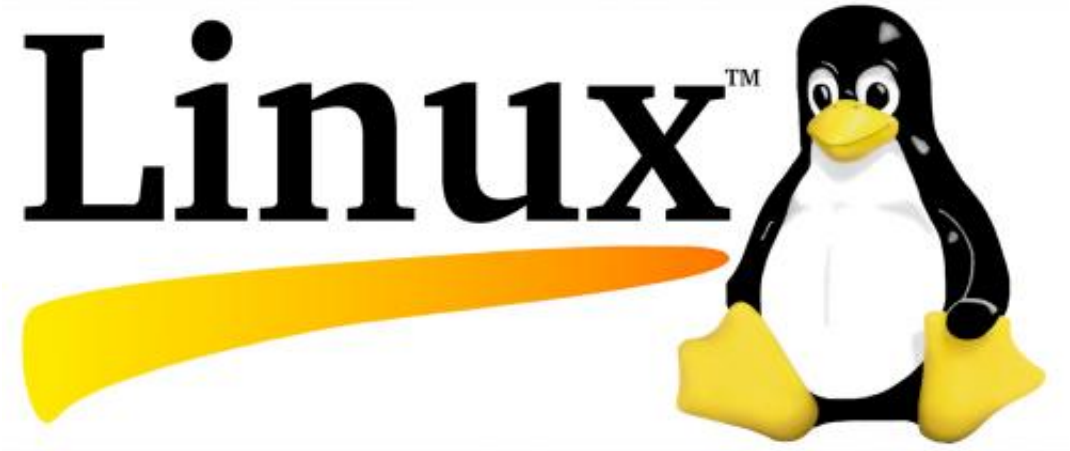
Red Hat programmer discovers major security flaw in Linux

March 6 2014, by Bob Yirka



(Phys.org) —Programmer Nikos Mavrogiannopoulos who works for Red Hat, has discovered a major security problem with the Linux operating system—a bug that could allow a hacker to create a certificate that could bypass the normal authenticity checks. Red Hat sent out an immediate alert and suggests all those who use its product update their software with a fix they've made available.

Officially known as CVE-2014-0092, the bug appears to be a simple

programming error—one that has been in a part of the Linux operating system for over a decade. More specifically, the bug involves GnuTLS's (a library of functions used for processing certificate requests) validation of X509 certificates. In many respects, the error appears to be similar to the "goto fail" security problem that cropped up in iOS and OS X recently. At issue in both cases is the infamous GOTO computer command which has been criticized by several high profile programmers for several years. Problems occur with it due to a programmer failing to consider one or more events. GOTO commands are called on demand, i.e. IF condition GOTO some other part of the code. The problem can be made worse if negative conditions are used because humans can't always think of every possible outcome.

In this instance, GOTO commands were being executed under certain conditions that allowed for bypassing certificate authentication, allowing unauthenticated certificates to be processed as if they were authentic. If a hacker discovered the flaw, they could cause their own certificates to be authenticated, allowing for decrypting data. That of course could impact a lot of users as Linux, especially the Red Hat version, is very commonly used as a web server operating system.

What is most surprising about the bug is that it went undetected for so long. Linux is an open source operating system which means thousands, if not millions, have access to the source code—every one of whom can test any part of it. That no one thought to independently test every part of the highly important GnuTLS's library seems almost unfathomable.

Now that the bug has been identified, fixes have been made in virtually all Linux variants, which users can download. Sadly, not everyone keeps up on such reports, however, which means the bug could very well live on in many web servers and others systems around the world for many years to come.

More information: rhn.redhat.com/errata/RHSA-2014-0246.html