Red Hat Risk Reflex (The Linux Security Flaw That Isn't)

By *Roy Schestowitz*
Created *10/03/2014 - 10:30am*
Submitted by Roy Schestowitz on Monday 10th of March 2014 10:30:19 AM Filed under Red Hat [1] Security [2]

News headlines screaming that yet another Microsoft Windows vulnerability has been discovered, is in the wild or has just been patched are two a penny. Such has it ever been. News headlines declaring that a 'major security problem' has been found with Linux are a different kettle of fish. So when reports of an attack that could circumvent verification of X.509 security certificates, and by so doing bypass both secure sockets layer (SSL) and Transport Layer Security (TLS) website protection, people sat up and took notice. Warnings have appeared that recount how the vulnerability can impact upon Debian, Red Hat and Ubuntu distributions. Red Hat itself issued an advisory warning that "GnuTLS did not correctly handle certain errors that could occur during the verification of an X.509 certificate, causing it to incorrectly report a successful verification... An attacker could use this flaw to create a specially crafted certificate that could be accepted by GnuTLS as valid." In all, at least 200 operating systems actually use GnuTLS when it comes to implementing SSL and TLS and the knock-on effect could mean that web applications and email alike are vulnerable to attack. And it's all Linux's fault. Or is it?

Read more ? [3]

Red Hat Security

Source URL: http://www.tuxmachines.org/node/64158

Links:
[1] http://www.tuxmachines.org/taxonomy/term/142
[2] http://www.tuxmachines.org/taxonomy/term/59
[3] http://www.daniweb.com/hardware-and-software/linux-and-unix/news/474947/red-hat-risk-reflex-the-linux-security-flaw-that-isnt