The Importance of Keeping PHP Up to Date

PHP is a robust and flexible language, used almost everywhere on the web in one form or another - and, increasingly, it's being used in many non-standard environments. As we grow into the so-called Internet of Things - the holy grail of web connectivity where every device we own is integrated into a network - the places PHP can be found are often extremely surprising to the unexpecting user. Never before has this been more highlighted than by a new piece of malware that was identified in the last two weeks by security firm Symantec.

Capitalising on a by now ancient PHP bug, the malware is a worm known as Linux.Darlloz has currently only been infected Intel x86-based systems, but security researchers warn that there are variants of the worms code that are designed for chip architectures that are most commonly found in consumer-grade routers, IP security cameras, and even television set-top boxes, which are not typically devices that are targeted by malware attacks. While there have been no recorded incidents of any of these devices being infected 'in the wild', the possibility exists that the current operational structure will change.

This serves to highlight the importance of working with up to date versions of PHP, and ensuring that if you or your company are responsible for working with devices that contain web interfaces, as most devices in the Internet of Things do for control and configuration purposes, it's absolutely crucial to roll out properly timed security updates. The particular flaw exploited by the Linux.Darlloz worm is only found in PHP versions 5.4.1 and earlier ; the patch for the flaw was implemented as far back as May 3rd of 2012.

It doesn't take much time to ensure that your current development environments are running the latest version of PHP - a quick version check and an update to your binaries is all it takes. It's possible that you may have to make some updates to any projects that are currently in the works, and if you've got any deployed projects they should be updated to patch any security flaws, but the benefits of the added stability and security far outweigh the hassles involved in staying updated. Even if you're not ready to adopt the latest bleeding edge version, at least try to stay with a version that was released in the current year.