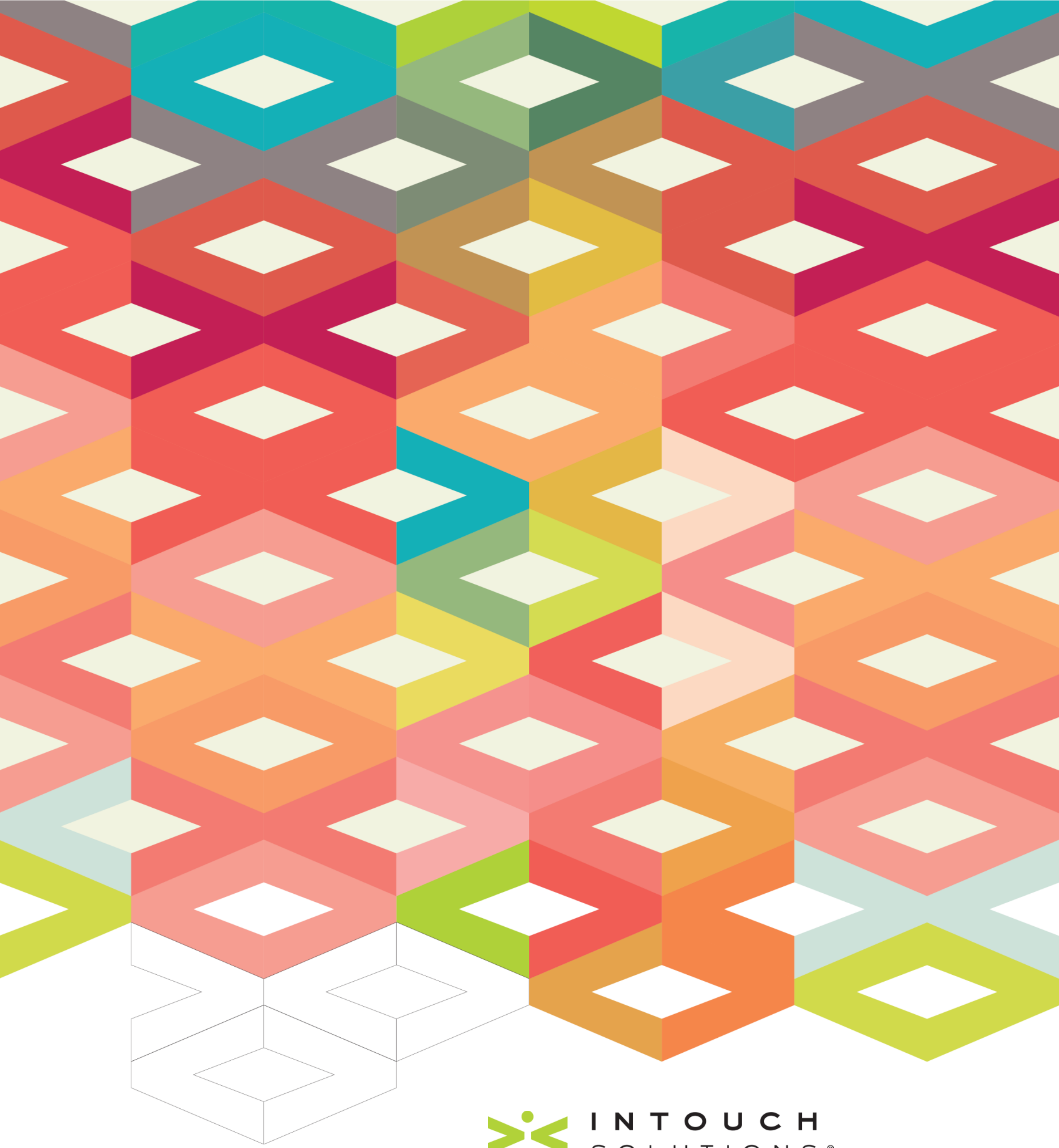

INTOUCH SOLUTIONS®

# **POV:** THE WORDPRESS BUG: WHAT YOU NEED TO KNOW

JANUARY 2015

proprietary

# WHAT THE WORDPRESS BUG MEANS FOR YOU AND HOW TO PROTECT YOUR SITES

## EXECUTIVE SUMMARY

A bug has been discovered that could affect up to 90 percent of WordPress websites and blogs, specifically those running versions 3.9.2 and earlier. The bug is very easily exploited; an attacker just has to enter malicious code into an open text field, such as a comment box, and the WordPress site or even the entire server could be compromised. The good news is the fix is easy. WordPress site managers need only upgrade to **the latest version of WordPress** and the site will be protected.

This POV describes in detail the WordPress bug security issues, implications and how to mitigage the vulnerability.

## WHAT IS THE WORDPRESS BUG?

This bug is a critical cross-site scripting vulnerability, which could enable anonymous users to compromise a site. Exploiting the bug is as simple as leaving a comment on a blog containing malicious code, which could allow a hacker to get administrative access to the server itself. With this level of access, the hacker could do basically anthing they wanted at the server level. To add insult to injury, hackers do not even have to log in to WordPress to leave the code — it can be done anonymously. Once the comment has been viewed by the blog admin's, the code gets to work taking over the account.

**Image Source**

This issue does not affect version 4.0, but **WordPress strongly encourages** immediately updating to version 4.0.1 — a critical security release — in order to address the following:

- Three cross-site scripting issues that a contributor or author could use to compromise a site
- A cross-site request forgery that could be used to trick a user into changing their password
- An issue that could lead to a denial of service when passwords are checked
- Additional protections for server-side request forgery attacks when WordPress makes HTTP requests
- An extremely unlikely hash collision could allow a user's account to be compromised if they haven't logged in since 2008 (which probably means it's not a critical blog for these folks)

It should also be noted that WordPress now invalidates the links in a password reset email if the user remembers their password, logs in and changes their email address.

## HOW IS THE BUG MITIGATED?

The WordPress team has released version 4.0.1, which addresses all known issues.

## WHAT HAS INTOUCH DONE TO MITIGATE THE WORDPRESS BUGS THAT IMPACT CLIENTS' WEBSITES? WHAT SHOULD CLIENTS DO?

Intouch Solutions has patched all WordPress servers with the latest version of WordPress in order to protect our sites and servers.

For clients, Intouch recommends verifying the version of any WordPress sites they have that are operational and always installing the latest version of software and security releases. Once again, this exploit highlights the importance of keeping WordPress sites and associated plugins up-to-date.

## WHAT DOES THE WORDPRESS BUG MEAN TO PHARMA/HEALTHCARE?

Though WordPress use is not as mainstream in pharma as in other industries, a number of pharmaceutical companies (including Intouch clients) do use WordPress for websites and blogs.

The biggest concern is, of course, patient information (PI). If PI was stored in the database, a hacker could potentially retrieve and exploit the data. One might assume that a site based on WordPress may not contain private information since it is labeled as a blogging engine. However, it has matured over the years into a simple, but effective, content management system used by millions of websites that are much more than blogs. Therefore, it needs to be treated and updated like any other site CMS.

## APPENDIX/REFERENCES

- WordPress bug leaves up to 90 percent of blogs at risk **by** Lisa Hoover McGreevy
- WordPress 4.0.1 Security Release **by** Andrew Nacin

*Author: Jeff Huggins, Director of Technology Strategy*