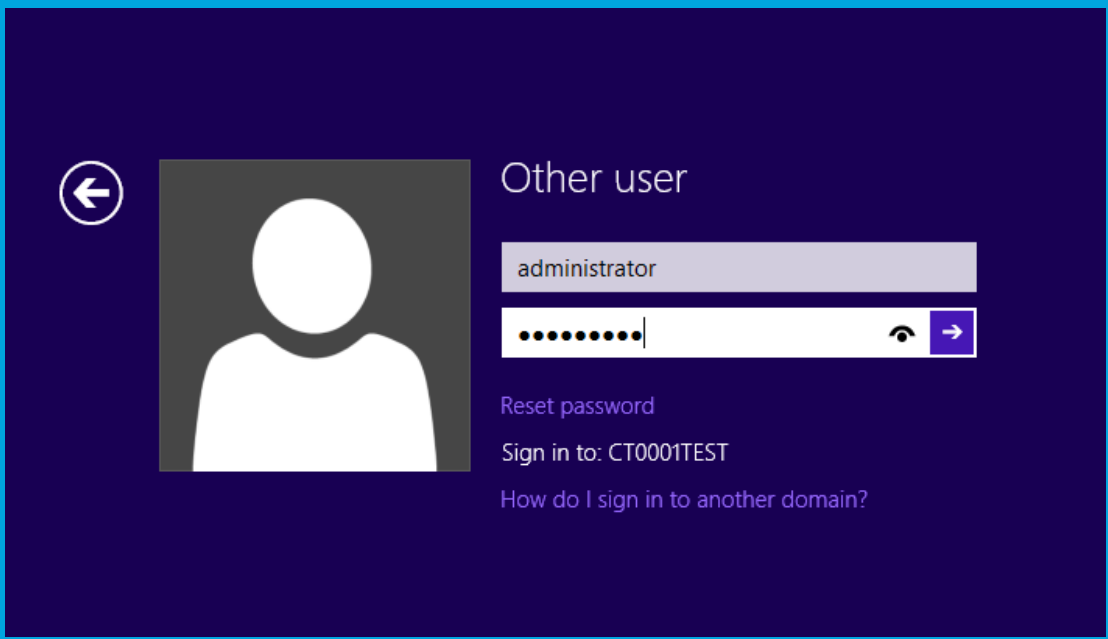
kindred

Security Newsletter

3 March 2017

Removing User Admin Rights Mitigates 94% of All Critical Microsoft Vulnerabilities!



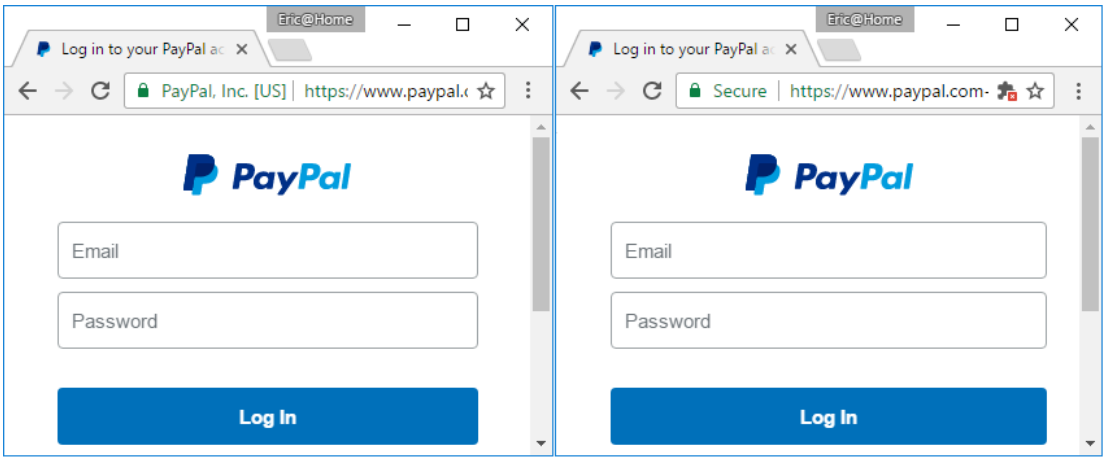
Just by preventing access to admin accounts, a system administrator could safeguard all the computers under his watch and prevent attackers from exploiting 94% of all the critical vulnerabilities Microsoft patched during the past year.

Even more interesting is that the Avecto 2016 report highlights that if sysadmins had forced users to utilize a low-privileged account instead of an admin-level profile, they would have mitigated 100% of all critical Internet Explorer and Microsoft Edge browser vulnerabilities patched during the past year.

What this growth from 86% to 94% means is that the security of Microsoft products is getting better, **if users would only start following industry best practices and stop using admin accounts for daily work.**

Read More

Phishing and HTTPS: Don't trust the "green lock"



One real, one fake, your account is at stake.

One unfortunate (albeit entirely predictable) consequence of making HTTPS certificates “fast, open, automated, and free” is that both good guys and bad guys alike will take advantage of the offer and obtain HTTPS certificates for their websites.

By December 8, 2016, LetsEncrypt had issued 409 certificates containing “Paypal” in the hostname; that number is up to 709 as of this morning. Other targets include BankOfAmerica (14 certificates), Apple, Amazon, American Express, Chase Bank, Microsoft, Google, and many other major brands.

We’ve had literally decades of sites and “experts” telling users to “Look for the lock!” when deciding whether a site is to be trusted. This has never been a reliable indicator, and this is now counter-productive. The "green lock" or the "secure" text on the left of the URL only means one thing: The connection between your browser and the server is encrypted. That’s it.

Read More

WordPress Plugin with over 1 Million installs Vulnerable to SQL Injection Attack

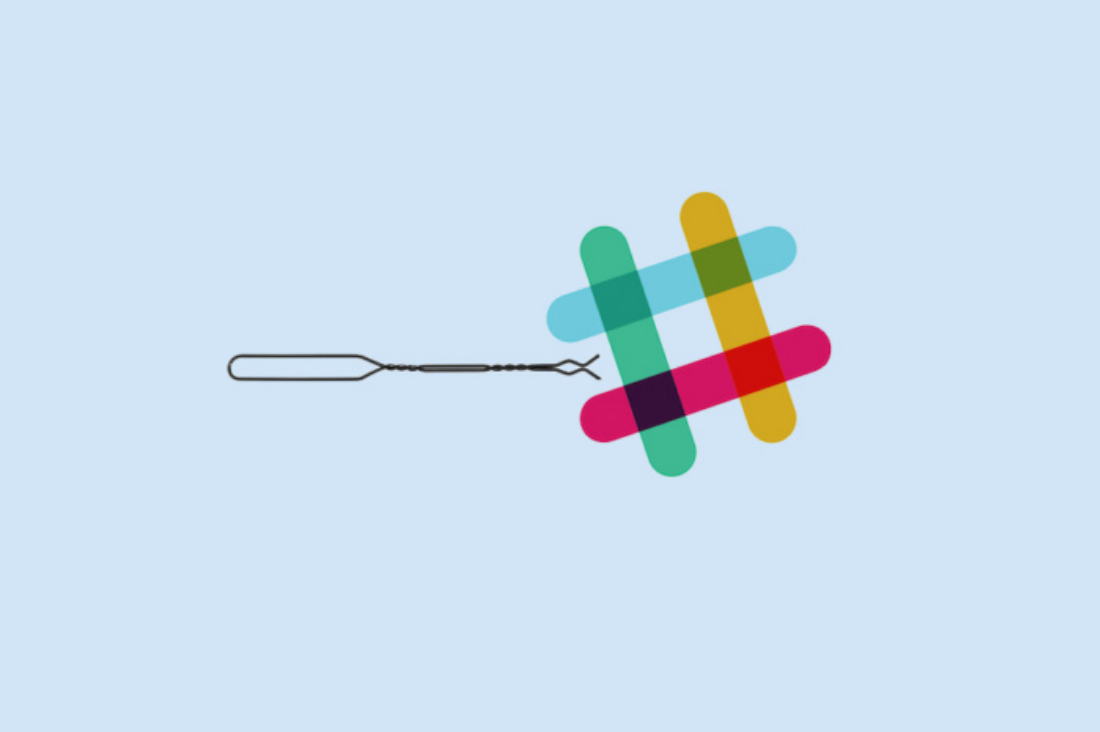
A web security firm- Sucuri discovered that the NextGen gallery for WordPress (WP) is affected by a severe SQL injection vulnerability and attackers can access the targeted website's database within minutes including all the sensitive data.

Although this is a vulnerability in WordPress plugin, the CMS itself is not much secure either. Last month security researchers at Sucuri discovered a severe content injection vulnerability in WordPress that would let attackers edit content on the WP based website.

It must be noted that days after the vulnerability was exposed hackers defaced thousands of WP websites. So in case, your are running a website on WP make sure to update your CMS to the latest version and same goes for the plugins.

Read More

Slack bug paved the way for a hack that can steal user access

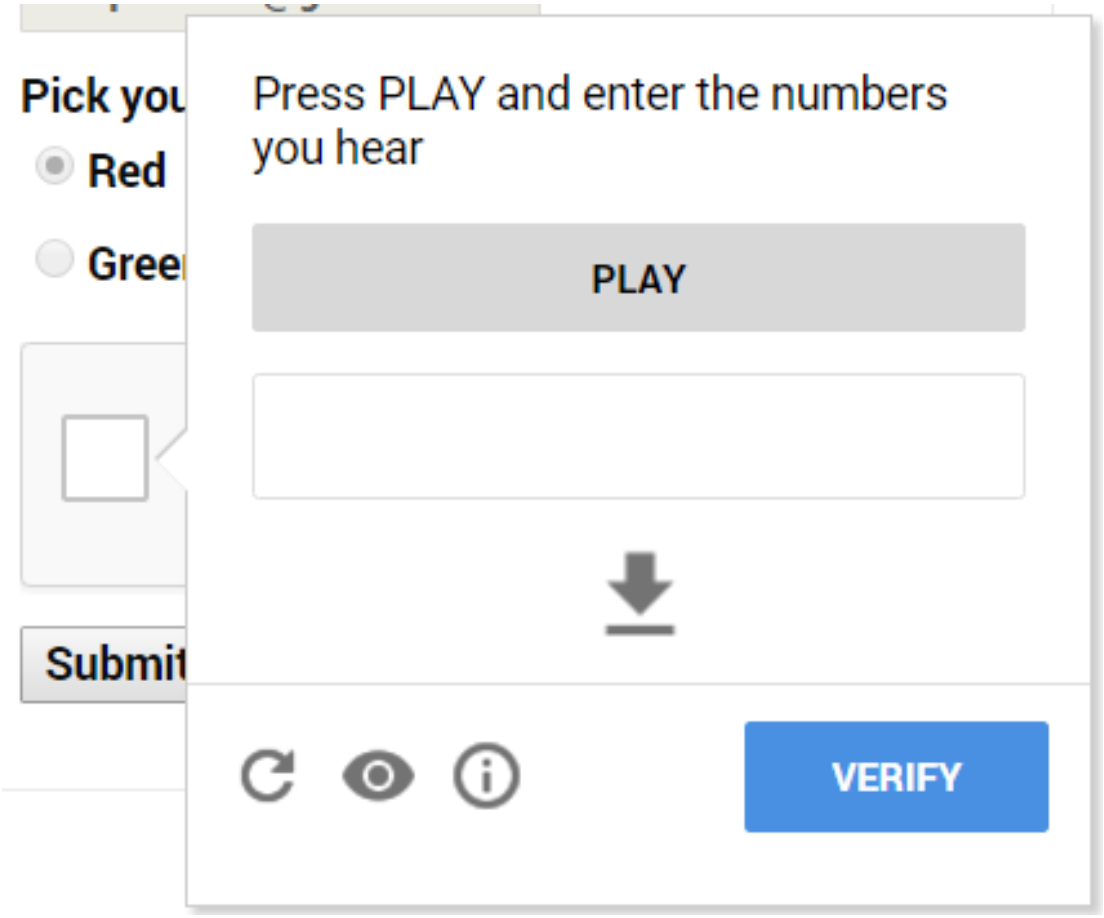


One bug in Slack, the popular work chat application, was enough for a security researcher to design a hack that could trick users into handing over access to their accounts.Bug bounty hunter Frans Rosen noticed he could steal Slack access tokens to user accounts due to a flaw in the way the application communicates data in an internet browser.

He demonstrated the theoretical hack in a video. The malicious webpage will open a Slack window that then forces a victim's account to handover its access token. Fortunately, Slack has now fixed the issue.

Read More

Researcher Breaks reCAPTCHA Using Google's Speech Recognition API



The attack is simple, but that doesn't mean that it is not capable. In very short terms, it takes the audio Captcha challenge from Google, runs it through Google's voice recognition technology and throws it back as a response.

This vulnerability is a good example of attackers always looking for the weakest link and targeting it. While Google standard CAPTCHA test is considered robust, the accessibility feature for people with visual impairment is weaker and that's what the hacker exploited.

Will the new Invisible ReCaptcha also find a way to solve this issue? We'll see!

Read More

AWS says a typo caused the massive 11-hours s3 failure this week

Other Amazon services in the US-EAST-1 region that rely on S3, like Elastic Block Store, Lambda, and the new instance launch for the Elastic Compute Cloud infrastructure-as-a-service offering were all impacted by the outage. The outage affected the likes of Netflix, Reddit, Adobe, and Imgur. More than half of the top 100 online retail sites experienced slower load times during the outage, website monitoring service Apica said.

As it turns out, Amazon hasn't fully restarted those systems in its larger regions for several years, and S3 has experienced massive growth in the intervening time.In response to this incident, AWS is making several changes to its internal tools and processes.

This event stresses out the importance of having multi-regions redundancy on critical cloud services.

Read More

Researchers Find 26 Security Flaws in 9 Popular Android Password Managers

While finding flaws in security tools is always worrying, please keep in mind that most of the high severity flaws require physical access to your smartphone to be exploited. Using this long, complex, unique passwords and storing them in this kind of encrypted vaults is still way better than relying on your memory alone, and hence falling back to short, simple, reused passwords to protect your accounts.

The list of tested apps includes MyPasswords, Informaticore, LastPass, Keeper, F-Secure Key, Dashlane, Hide Pictures Keep Safe Vault, Avast Passwords, and 1Password. All tested apps were installed on at least 500,000 devices, with some apps having millions of users.

All found issues have now been fixed.

Read More

This content was created by Kindred Group Security. Please share if you enjoyed!

Kindred Group in brief

Kindred is one of the largest online gambling companies in the world with over 15 million customers across 100 markets. We offer pre-game and live Sports betting, Poker, Casino and Games through 13 subsidiaries and brands across our markets. We are committed to offer our customers the best deal and user experience possible, while ensuring a safe and fair gambling environment. Kindred is a pioneer in the online gambling industry and as an innovation driven company that builds on trust.