The Hacker News™
Security in a serious way

WordPress Security: Brute Force Amplification Attack Targeting Thousand of Blogs

Friday, October 09, 2015 Swati Khandelwal

Most of the times, we have reported about WordPress vulnerabilities involving vulnerable plugins, but this time security researchers have discovered **Brute Force Amplification attacks** on the most popular CMS (content management system) platform.

Researchers from security firm Sucuri have found a way to perform Brute Force amplification attacks against WordPress' built-in **XML-RPC feature** to crack down administrator credentials.

XML-RPC is one of the simplest protocols for securely exchanging data between computers across the Internet. It uses the **system.multicall** method that allows an application to execute multiple commands within one HTTP request.

A number of CMS including WordPress and Drupal support XML-RPC.

But…

The same method has been abused to amplify their Brute Force attacks many times over by attempting hundreds of passwords within just one HTTP request, without been detected.

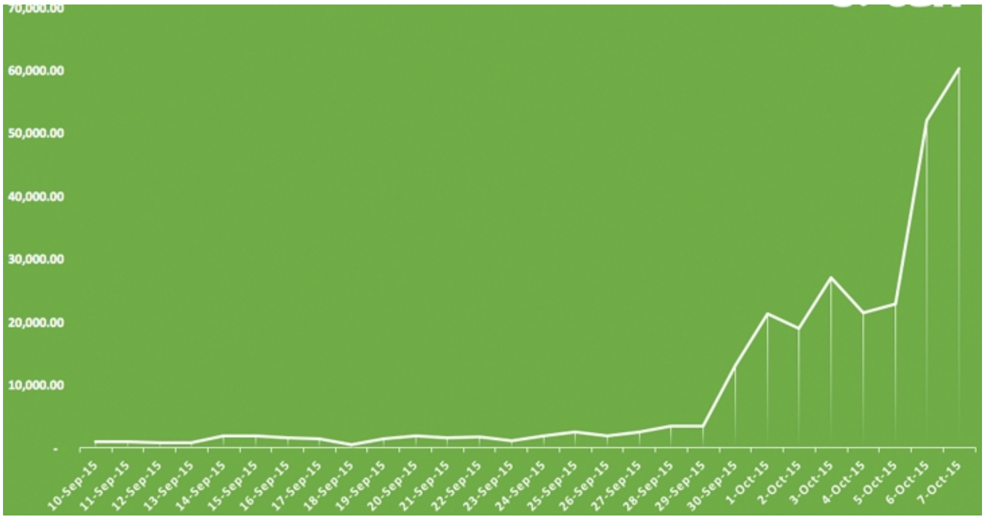
Amplified Brute-Force Attacks

This means instead of trying thousands of usernames and password combinations via login page (which can be easily blocked by banning IPs), hackers can use the **XML-RPC** protocol in conjunction with the **system.multicall** method that allows them to:

- Go undetected by normal brute-force mitigation products
- Try hundreds of thousands of username and password combinations with few XML-RPC requests.

> *"With only 3 or 4 HTTP requests, the attackers could try thousands of passwords, bypassing security tools that are designed to look and block brute force attempts,"* Sucuri's researchers wrote in a blog post.

The company witnessed the first attack of this kind at the beginning of last month, which then sky-



rocketed to around **60,000 per day** by the start of this month.

How to Prevent Brute-Force Amplification Attack via XML-RPC

To protect yourself against such threat, simply block all access to XML-RPC.

If you are not using any plugin that uses the xmlrpc.php file, just head on to rename/delete it. But, if you are using plugins such as **JetPack**, blocking xmlrpc.php may result in some broken functionality on your website.

So, webmasters could block XML-RPC system.multicall requests using a WAF (web application firewall). This will protect you against the amplification methods.

Brute Force Attack, Hacking News, Password Cracker Software, Vulnerability, WordPress Exploit, Wordpress Hacking, Wordpress Security, WordPress Vulnerability

ABOUT THE AUTHOR

Swati Khandelwal

Senior Technical Writer at Hacker News. Social Media Lover and Gadgets Girl. Speaker, Cyber Security Expert and Technical Writer.

ALIEN VAULT
INSIDER'S GUIDE TO INCIDENT RESPONSE
GET OUR NEW INSIDER'S GUIDE TO
INCIDENT RESPONSE ›

WANT MORE STUFF LIKE THIS?

Want more Interesting News like this? Sign up here to receive the best of 'The Hacker News' delivered daily straight to your inbox.

Email address

Subscribe

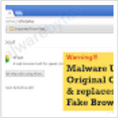
LATEST STORIES

Cracking WiFi Passwords By Hacking into Smart Kettles

Here's How SIEM Can Protect Your Privileged Accounts in the Enterprise

Google Makes Full-Disk Encryption Mandatory for New Android 6.0 Devices

More than 250 iOS Apps Caught Using Private APIs to Collect Users' Private Data


This Malware Can Delete and Replace Your Entire Chrome Browser with a lookalike

High school Student Hacked Into CIA Director's Personal Email Account

How to Protect Yourself against XcodeGhost like iOS Malware Attacks

Facebook Will Now Notify You If NSA is Spying on You

COMMENTS

0 Comments The Hackers News 1 Login

Recommend Share Sort by Newest

Start the discussion…

Be the first to comment.

ALSO ON **THE HACKERS NEWS** WHAT'S THIS?

Microsoft doesn't want Windows 10 Users to Switch to Chrome or Firefox

13 comments • 2 days ago

droopyar — i love firefox

High school Student Hacked Into CIA Director's Personal Email Account

13 comments • a day ago

richardstevenhack — I think we can assume that the CIA Directory had no classified data in his AOL account. My guess is the data this guy …

This 'Radio Wave' Hack allows Hackers to Control Your Phone From 16 Feet Away

3 comments • 7 days ago

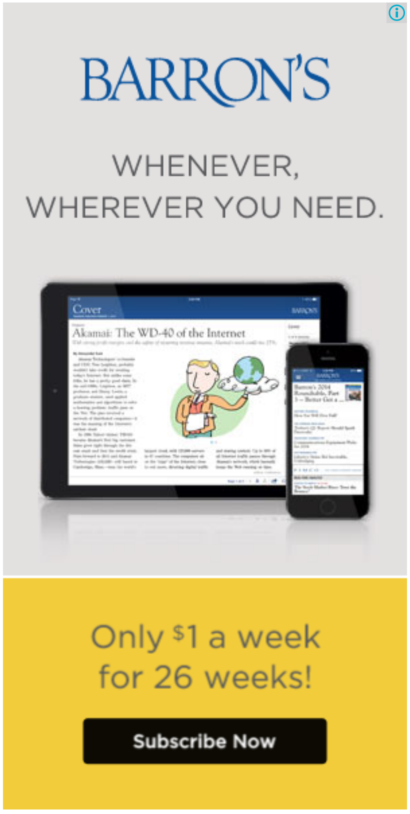
NoName — I've known of this for some time. There is MUCH exploitable features. Now I 100% DISAGREE and KNOW for a FACT. This can …

This Malware Can Delete and Replace Your Entire Chrome Browser with a lookalike

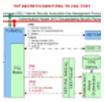
2 comments • a day ago

Jake Myers — Does it replicate your extension icons or bookmark bars?

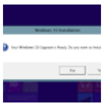
Subscribe Add Disqus to your site Privacy DISQUS



Popular Stories


How NSA successfully Broke Trillions of Encrypted Connections

First Ever Anti-Drone Weapon that Shoots Down UAVs with Radio Waves


Windows 10 Upgrade Become More Creepy, No Option to Opt-Out

High school Student Hacked Into CIA Director's Personal Email Account

Hackers Can Use Radio-waves to Control Your Smartphone From 16 Feet Away

Facebook Will Now Notify You If NSA is Spying on You

This Guy Builds A Thor-Like Hammer that Only He Can Pick Up

ISIS Hacker who Passed U.S. Military Data to Terrorists Arrested in Malaysia

About | THN Magazine | The Hackers Conference | Sitemap | Advertise on THN | Submit News | Privacy Policy | Contact