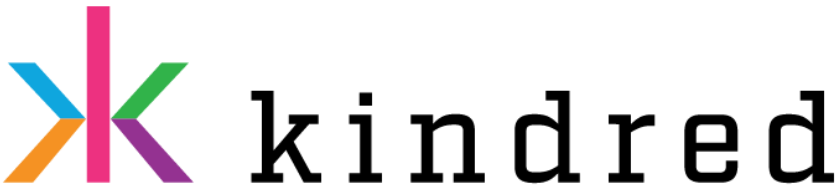

Security Newsletter

9 April 2018

Subscribe to this newsletter

Remote Execution Flaw Threatens Apps Built Using Spring Framework — Patch Now

Security researchers have discovered three vulnerabilities in the Spring Development Framework, one of which is a critical remote code execution flaw that could allow remote attackers to execute arbitrary code against applications built with it. Spring Framework is a popular, lightweight and an open source framework for developing Java-based enterprise applications.

Vulnerable Spring Framework versions expose STOMP clients over WebSocket endpoints with an in-memory STOMP broker through the 'spring-messaging' module, which could allow an attacker to send a maliciously crafted message to the broker, leading to a remote code execution attack (CVE-2018-1270).

The second bug (CVE-2018-1271) resides in Spring's Web model-view-controller (MVC) that allows attackers to execute directory traversal attack and access restricted directories when configured to serve static resources (e.g., CSS, JS, images) from a file system on Windows. This vulnerability doesn't work if you are not using Windows to serve content and can be avoided if you don't serve files from the file system or use Tomcat/WildFly as the server.

Pivotal has released Spring Framework 5.0.5 and 4.3.15, which include fixes for all the three vulnerabilities. The company has also released Spring Boot 2.0.1 and 1.5.11, that match the patched Spring Framework versions. So developers and administrators are highly recommended to upgrade their software to the latest versions immediately.

Read More

Advisory

Magento sites hacked with cryptominers & credential stealing malware

Security researchers say they've identified at last 1,000 Magento sites that have been hacked by cybercriminals and infected with malicious scripts that steal payment card details or are used as staging points in the delivery of other malware.

The Magento sites are being compromised through brute-force attacks using common and known default Magento credentials, brute-force attacks such as these are simplified when admins fail to change the credentials upon installation of the platform. Attackers, meanwhile, can build simple automated scripts loaded with known credentials to facilitate access of the panels.

In today's cybercrime landscape where criminals have access to cheap brute-forcing botnets that they can use to guess site passwords with relatively little effort, site owners should make sure they use unique usernames and passwords that can't be guessed after a few attempts. Securing admin account passwords should be a top priority —next to applying security updates— for all site owners, not just those managing online stores.

Read More

How to recover a hacked Magento shop

Security Experts Weigh In On Massive Data Breach Of 150 Million MyFitnessPal Accounts

Under Armour has admitted that around 150 million MyFitnessPal user accounts were hacked in February of this year. MyFitnessPal is a popular fitness tracking app that has been around for a long time. It was founded in 2005 and enables users to monitor calorie intake and exercise. Under Armour acquired MyFitnessPal about three years ago for $475 million.

A post on the MyFitnessPal site shares the details known so far and offers some guidance for affected users. It explains that Under Armour is notifying all MyFitnessPal users to provide information about how to protect their data, requiring all users to change their passwords, working with law enforcement to investigate and continuing to monitor for suspicious activity, and exploring enhancements to help detect and prevent similar unauthorized access in the future.

The good news for those affected is that the only data that was exposed or potentially compromised was usernames, email addresses, and encrypted passwords. More sensitive—and potentially more harmful—data like Social Security numbers or driver's license numbers are not collected by MyFitnessPal, and the bank and credit card details are collected and processed separately. Under Armour states that most of the passwords were encrypted with bcrypt—which is a relatively strong password hashing mechanism. However, some of the passwords were protected using a significantly weaker 160-bit hashing function, SHA-1.

Read More

Official advisory

Patches, leaks, releases and the kitchen sink

- LiveChat widgets vulnerability allow leaking details of employees
- AWS Secrets Manager: Store, Distribute, and Rotate Credentials Securely
- VirusTotal Launches Droidy, Its New Android Sandbox Technology
- Facebook admits public data of its 2.2 billion users has been compromised
- Microsoft Out-Of-Band Security Update Patches Malware Protection Engine Flaw
- New macOS malware aims at infecting devices with malicious macros
- Misconfigured Django Apps Are Exposing Secret API Keys, Database Passwords
- Mad March Meltdown! Microsoft's patch for a patch for a patch may need another patch
- Grindr is revealing its users' HIV status to third-party companies
- Microsoft Out-Of-Band Security Update Patches Malware Protection Engine Flaw
- Panera Bread customer records exposed via leaky database – dough!

Tech content and tools

- Whonow: "malicious" DNS server for executing DNS Rebinding attacks on the fly
- Zero-width steganography PoC
- Expand your horizon, read teams – Modern SaaS C2
- CloudFront Hijacking
- Hakluke's Ultimate OSCP Guide: Part 3 — Practical hacking tips and tricks
- On-site Request Forgery
- Your website needs a CSP, here's why
- Introducing the CSP Wizard on Report URI
- Organisations, don't underestimate DMARC policy!
- Your website has assets, use SRI

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.