ИТМО

Критическая уязвимость в Java-фреймворке Spring (Spring4Shell)

Неграш А.В., P33301

Spring4Shell. Начало

ИТМО

31 марта 2022

9.8
(Critical)

VMware публикует отчёт об уязвимости CVE-2022-22965

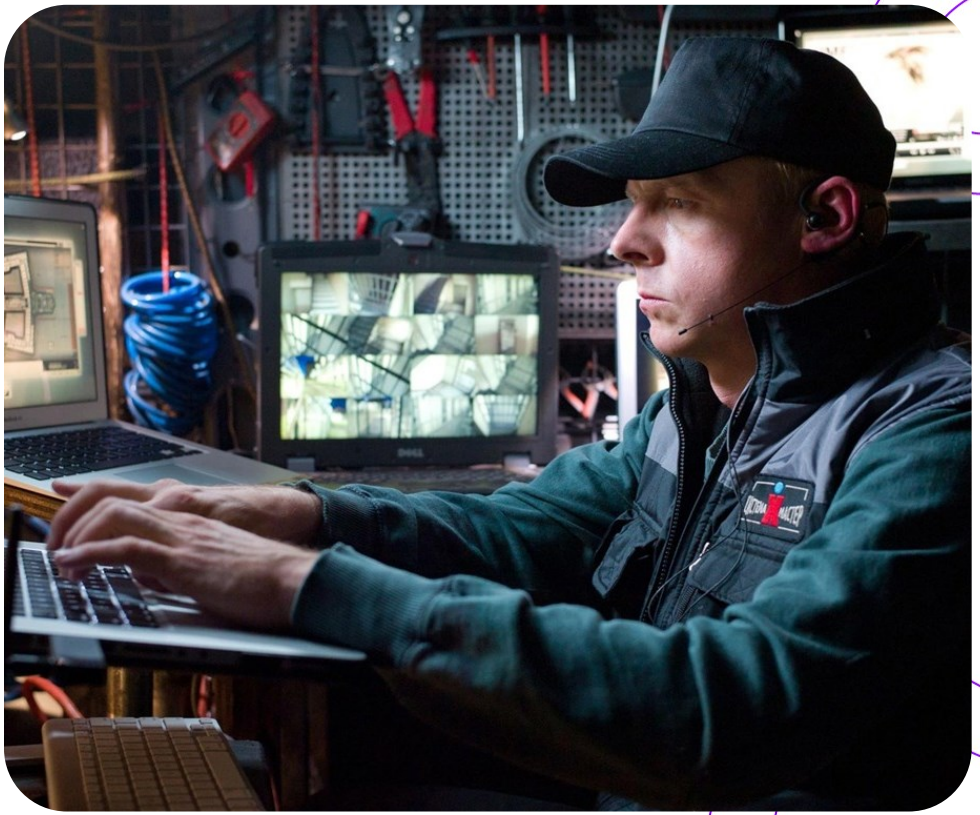
Ссылка на статью

RCE-уязвимость

Remote **C**ode **E**xecution – уязвимость, при которой можно выполнить произвольный код в целевой системе без физического подключения.

RCE-уязвимости по статистике получают наибольший рейтинг по системе Common Vulnerability Scoring System

Интересный факт



В фильме **«Миссия невыполнима: Протокол Фантом»** для выполнения подключения к спутнику связи использовали “уязвимость на управляющем сервере”.

Судя по контексту, это была **RCE-уязвимость.**

Кто поражён

ИТМО

Java Development Kit 9+

Apache Tomcat

WAR-файлы

Использование spring-webmvc или spring-webflux

Spring Framework 5.3.0 … 5.3.17, 5.2.0 … 5.2.19 и старше

Процесс атаки

ИТМО

1. POST-запрос с параметрами
   class.module.classLoader.resources.context.parent.pipeline.first.pattern=<вредоносный java-код>
   class.module.classLoader.resources.context.parent.pipeline.first.prefix=bad-script
   class.module.classLoader.resources.context.parent.pipeline.first.suffix=.jsp

2. Обращение по адресу **/bad-script.jsp** через терминал или просто в браузере и выполнение желаемых действий

ДИСКЛЕЙМЕР

Данная информация приведена исключительно в ознакомительных целях, я призываю не использовать эти знания для совершения противоправных действий

Как защититься?

ИТМО

Обновить Spring Framework до версий
5.3.18 и **5.2.20** или новее

Ваш К.О.

Как защититься?

ИТМО

Понизить JDK до 8 версии

- ➕ Надёжно
- ➕ Быстро
- ➖ Временное решение
- ➖ Сложности для больших проектов

Запретить POST-запросы, содержащие атрибут «class»

- ➕ Быстро
- ➕ Без конфликтов
- ➖ Костыли
- ➖ Неполная защита от уязвимости

Мораль

- ~~Разработчикам надо лучше тестировать свои продукты, чтобы не было RCE-уязвимостей~~
- Использовать сторонние библиотеки с умом и в необходимо умеренном количестве
- Следить за официальными каналами оповещения для продуктов, которые используете

Спасибо
за внимание!

ITMO more than a UNIVERSITY

Неграш Андрей, P33301
anegrash@nav-com.ru