紧急通知

鉴于公司多数同事们采用spring框架来进行开发，下面对一些spring框架nday漏洞进行简单普及，大家根据自己的项目进行自查。

**1.Spring WebFlow**

漏洞编号：CVE-2017-4971

受影响版本：**spring-web flow 2.4.0-2.4.4**

漏洞危害：远程代码执行

修复建议：参考<https://tanzu.vmware.com/security/cve-2017-4971，或者自行百度/>谷歌

**2.SPRING DATA REST**

漏洞编号：CVE-2017-8046

受影响版本

* **Spring Data REST versions < 2.5.12, 2.6.7, 3.0 RC3**
* **Spring Boot version < 2.0.0M4**
* **Spring Data release trains < Kay-RC3**

危害：远程代码执行

修复建议：<https://tanzu.vmware.com/security/cve-2017-8046>

**3.spring-messaging组件**

漏洞编号：CVE-2018-1270

受影响版本：

* **Spring Framework 5.0 to 5.0.4**
* **Spring Framework 4.3 to 4.3.15**
* **早期官方已不支持的版本**

**使用了该组件的员工建议网上查阅自测**

漏洞危害：远程代码执行

修复建议：https://tanzu.vmware.com/security/cve-2018-1275

**4.SPRING DATA COMMONS**

漏洞编号：CVE-2018-1273

受影响版本：

* **Spring Data Commons 1.13 – 1.13.10 (Ingalls SR10)**
* **Spring Data REST 2.6 – 2.6.10(Ingalls SR10)**
* **Spring Data Commons 2.0 – 2.0.5 (Kay SR5)**
* **Spring Data REST 3.0 – 3.0.5(Kay SR5)**
* **官方已经不支持的旧版本**

危害：远程代码执行

修复建议：<https://tanzu.vmware.com/security/cve-2018-1273>

**5.Spring Cloud Gateway远程代码执行**

漏洞影响版本：

* **Spring Cloud Gateway<3.1.1**
* **Spring Cloud Gateway<3.0.7**
* **Spring Cloud Gateway其他已不再更新的版本**

修复建议：https://tanzu.vmware.com/security/cve-2022-22947