漏洞介绍

漏洞名称	**Vmware Spring Framework 代码注入漏洞**
漏洞等级	超危
漏洞类型	代码注入
CVE编号	CVE-2022-22965
CNNVD编号	CNNVD-202203-2642
漏洞简介	Vmware Spring Framework是美国威睿（Vmware）公司的一套开源的Java、JavaEE应用程序框架。 该框架可帮助开发人员构建高质量的应用。Vmware Spring Framework 存在代码注入漏洞，该漏洞源于 JDK 9+ 上的数据绑定的 RCE。
修复方案	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://tanzu.vmware.com/security/cve-2022-22965

漏洞特征

Payload/uri中包含下面特征

```
class.module.classLoader.URLS[0]=0
class.module.class.module.class.module.classLoader.
class.classLoader.resources.context.parent.pipeline.first.pattern
class.classLoader.resources.context.parent.pipeline.first.directory
class.classLoader.resources.context.parent.pipeline.first.prefix
class.classLoader.resources.context.parent.pipeline.first.suffix
class.classLoader.resources.context.parent.pipeline.first.fileDateFormat
```

相关规则

可以将规则添加到Post/Get过滤中，但是添加后发现无法保存

```
(class.classLoader.resources.context.parent.pipeline.first.pattern|class.classLoader.resources.context.parent.pipeline.first.directory|class.classLoader.resources.context.parent.pipeline.first.prefix|class.classLoader.resources.context.parent.pipeline.first.suffix|class.classLoader.resources.context.parent.pipeline.first.fileDateFormat|class.module.classLoader.URLS[0]=0|class.module.class.module.class.module.classLoader)
```