

漏洞描述

漏洞URL：如果是Web就填写此项

https://api.v****.cc/druid/index.html

简要描述：漏洞说明、利用条件、危害等

https://api.v****.cc/druid/index.html

Druid未授权访问，泄露部分敏感信息

漏洞证明：

此处可找到找到api接口地址： https://api.****.cc/



存在Druid接口未做访问控制： https://api.*****.cc/druid/index.html



DataSourceStat List View JSON API

DataSource-7732389

Basic Info For DataSource-7732389 View JSON API

* 用户名	vbexchangeuser	指定建立连接时使用的用户名
* 连接地址	jdbc:mysql://api.*****.cc:3306/?useUnicode=true&characterEncoding=utf-8	jdbc连接字符串
* 数据库类型	mysql	数据库类型
* 驱动类名	com.mysql.jdbc.Driver	jdbc驱动类名
* filter类名	com.alibaba.druid.filter.stat.StatFilter	filter的类名
* 获取连接时检测	false	是否在获得连接后检测其可用性
* 空闲时检测	true	是否在连接空闲一段时间后检测其可用性



Stat Index [查看JSON API](#)

版本	1.0.19
驱动	com.alibaba.druid.mock.MockDriver com.mysql.jdbc.Driver com.mysql.fabric.jdbc.FabricMySQLDriver com.alibaba.druid.proxy.DruidDriver
是否允许重置	true
重置次数	0
java版本	1.8.0_275
jvm名称	OpenJDK 64-Bit Server VM
classpath 路径	/mnt/.../api/lib/jedis-2.8.1.jar /mnt/.../api/lib/javax.servlet-api-3.1.0.jar /mnt/.../api/lib/aspectjweaver-1.8.9.jar /mnt/.../api/lib/spring-orm-4.2.6.RELEASE.jar /mnt/.../api/lib/spring-aop-4.2.6.RELEASE.jar

Druid Monitor													
URI监控													
N	URI	请求次数	请求时间	中	发	数	数	Jdbc时间	数	数	读取行数	更新行数	[-----]
1	/errc	2			1								[2,0,0,0,0,0,0]
2	/dr	1	1		1								[0,1,0,0,0,0,0]
3	/api/v1/	20	1,155		1	40		182			20	20	[0,0,20,0,0,0,0]
4	/api/	26,201	1,728,582		3	97,458		1,428,256			1,523,228		[0,39,24377,1596,186,3]
5	/api/	4,240,496	432,513,987	1	33	27,543,111		109,206,117			20,136,033	6,337,774	[0,141,2692125,154360]
6	/api/v	429	283		1								[428,1,0,0,0,0,0]
7	/api/	981,079	291,628		3								[980165,910,1,3,0,0,0]
8	/api/v	3,930,854	5,342,894		5								[50185,3880596,69,4,0]
9	/api/v1/	14,320	659,014		1	14,320		515,281					[0,0,14158,162,0,0,0]
10	/	14,342	601,266		1	14,342		457,026			6		[0,0,14215,127,0,0,0]
11	/ap	14,339	657,633		1	14,339		512,361			310		[0,0,14183,156,0,0,0]
12		1,522,663	570,208		5								[1519528,3132,0,3,0,0]

漏洞利用代码：

https://api.**.cc/druid/index.html

修复方案：

做访问控制

漏洞总结

Druid是阿里巴巴出品，为监控而生的数据库连接池。Druid提供了监控功能，如监控SQL的执行时间、监控Web URI的请求、Session监控，当开发者配置不当时可能造成未授权访问

以下为druid常见的web路径，如果可直接访问到相关页面，说明存在Druid未授权访问

/druid/websession.html

/system/druid/websession.html

/webpage/system/druid/websession.html