# 绿盟科技安全预警通告

Weblogic WLS 组件漏洞攻击利用预警

预警编号	NS-2017-0030
漏洞编号	CVE-2017-10271
CVSS v3 评分	9.8 Critical
	(CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
影响版本	Oracle WebLogic Server;
	version: 10.3.6.0.0, 12.1.3.0.0, 12.2.1.1.0, 12.2.1.2.0.
TAG	Weblogic、CVE-2017-10271、wls-wsat、远程代码执行、 挖矿程序;

WebLogic WLS 组件漏洞攻击利用安全预警



# -. 预警摘要

近期,绿盟科技应急响应团队陆续接到来自金融、运营商、互联网等多个行业客户的安 全事件反馈,发现多台不同版本 WebLogic 主机均被植入了相同的恶意程序,该程序会消耗大 量的主机 CPU 资源。

经分析,攻击者针对 WebLogic WLS 组件中存在的 CVE-2017-10271 远程代码执行漏洞,构造请求对运行的 WebLogic 中间件主机进行攻击,由于该漏洞利用方式简单,且能够直接获取目标服务器的控制权限,影响范围较广,近期发现此漏洞的利用方式为传播虚拟币挖矿程序,不排除会被黑客用于其他目的的攻击。

Oracle 官方网站在 10 月份的更新补丁中对此漏洞进行了修复,建议企业做好安全防护措施,并及时修复,减少因此漏洞造成的损失。官方修复详情参考如下链接:

http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html

# 二. 安全防护

由于攻击者利用的是 WebLogic wls 组件进行的攻击,当 WebLogic 控制台对公网开放且 未及时升级安全补丁的话,就会存在被利用的风险。

## 2.1 官方升级方案

Oracle 官方对于 WebLogic WLS 组件漏洞(CVE-2017-10271)在 10 月份的更新补丁中已 经进行了修复,建议及时下载更新包,并升级 WebLogic。升级过程可参考如下链接:

http://blog.csdn.net/qqlifu/article/details/49423839

## 2.2 临时防护建议

根据攻击者利用 POC 分析发现所利用的为 wls-wsat 组件的 CoordinatorPortType 接口, 若 Weblogic 服务器集群中未应用此组件,建议临时备份后将此组件删除,当形成防护能力后, 再进行恢复。

**NSFOCUS** 

1. 根据实际环境路径,删除 WebLogic wls-wsat 组件:

rm -f /home/WebLogic/Oracle/Middleware/wlserver\_10.3/server/lib/wls-wsat.war rm -f

/home/WebLogic/Oracle/Middleware/user\_projects/domains/base\_domain/servers/AdminServer/tmp/.internal/wls-wsat.war

rm -rf

/home/WebLogic/Oracle/Middleware/user\_projects/domains/base\_domain/servers/AdminServ er/tmp/\_WL\_internal/wls-wsat

**2.** 重启 Weblogic 域控制器服务。

DOMAIN\_NAME/bin/stopWeblogic.sh #停止服务 DOMAIN\_NAME/bin/startManagedWebLogic.sh #启动服务

关于重启 Weblogic 服务的详细信息,可参考如下官方文档:

https://docs.oracle.com/cd/E13222\_01/wls/docs90/server\_start/overview.html

# 2.3 产品防护方案

## 2.3.1 WAF 防护方案

部署有绿盟科技 WAF 的用户可通过自定义规则的方式用来及时防护 WebLogic WLS 组件远程代码执行漏洞,自定义规则如下:

(uri \* rco /wls-wsat/CoordinatorPortType)&&(request\_body \* rco (?is)(<object|<new|<method|<void\s+[^>]\*(method|class)\s\*=))

配置效果如下图所示:

<sup>™</sup> NSFOCUS		WebLogic WLS 组件漏洞攻击利用安全
告警 <del>类型</del> 检测方向	自定义	▼
设置约束条件	检测对象 匹配操作 检测值 🕢	Request-Body ▼ 正则包含 ▼ \s+[^>]*(method class)\s*=) 区分大小写
		添加移除
约束条件	(uri * rco /wls-wsa ( <object <new <n< th=""><th>at/CoordinatorPortType)&amp;&amp;(request_body * rco (?is) nethod <void\s+[^>]*(method class)\s*=))</void\s+[^></th></object <new <n<>	at/CoordinatorPortType)&&(request_body * rco (?is) nethod  <void\s+[^>]*(method class)\s*=))</void\s+[^>

WAF 自定义规则防护过程可参考附录 A。

# 2.3.2 NIPS 防护方案

部署有绿盟科技 NIPS/NIDS 的用户,可通过自定义规则,形成对 WebLogic WLS 组件远 程代码执行漏洞利用的检测和防护。配置信息如下表所示:

名称	weblogic_wls_wsat
级别	根据实际需要进行配置
协议类型	ТСР
目的端口	Weblogic 服务的端口,默认为 7001,根据实际部署情况确定端口
关键字	regex*wls-wsat\/CoordinatorPortType.*([ <void <new method <object class]?)+.*< th=""></void <new method <object class]?)+.*<>

效果如下图所示:

预嚐

MSFOCUS

#### WebLogic WLS 组件漏洞攻击利用安全预警

夕称 🖌	weblogic wis weat		
-1113- 1	规则名称是规则的唯一标识,	不可重复命名	
级别	◎ 低风险事件 🔘 中风险事	6件 💿 高风险事件	
匹配范围	◉ 单包匹配		
协议类型	TCP ▼ 以下几项内容不能	能全部为空	
源端口		范围为0~65535	
目的端口	7001	范围为0~65535	
包长度		范围为0~65535	
关键字	regex*wls-wsatVCoordinat <new method <object class]< th=""><th>orPortType.*([<void] ?)+.*</void] </th><th>Ø</th></new method <object class]<>	orPortType.*([ <void] ?)+.*</void] 	Ø

详细配置过程参考附录 B。

# 三. 感染主机排查

由于此次攻击主要目的为下载执行挖矿程序,从主机层面可通过监控主机系统资源或进程分析方式进行检测,从网络层面可对 C&C 地址及矿池相关域名/IP 进行监控,以发现其他受感染主机。

# 3.1 主机层面排查

针对 linux 主机,首先查看/tmp 目录中是否存在属主为 WebLogic 运行账户的相关可疑文件,如:watch-smartd、Carbon、default。

* 20 L	-	-			-
			_	_	-

[root@1/2-1-2-88 ~]#  s - s /tmp/	
total 2240	
4 drwxr-x 2 tomcat tomcat 4096 Dec 20 02:48 hsperroata_tomcat	
4 drwxr 2 weblogic bea 4096 Dec 20 02:48 hsperfdata_weblogi	
2224 -rwxrr 1 weblogic bea 2274080 Dec 19 21:13 watch-smartd	
4 druxr-xx 3 root for all 23:47 wist ampropt	
4 drwxr-xx 3 weblogic bea 4096 Oct 31 09:31 wistTempweblogic	
[root@172-1-2-88 ~]# ps -ef  grep watch	
root 6 2 0 02:47 ? 00:00:00 [watchdog/0]	
weblogic 1832 1 0 17:37 ? 00:00:00 ./watch-smartd -B	
root 1852 1814 0 17:43 pts/1 00:00:00 grep watch	
[root@172-1-2-88 ~]#	

通过进程及系统资源分析,确认是否存在启动用户为 WebLogic 运行账户的相关可疑进

程。

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+ COMMAND
1099	weblogic	20	0	1550m	360m	40m	S	0.0	19.2	1:37.93 java
1100	weblogic	20	0	1559m	345m	44m	s	1.3	18.5	2:20.81 java
1062	tomcat	20	0	2435m	89m	13m	s	0.0	4.8	1:09.17 java
1753	root	20	0	99.2m	5700	3420	S	0.0	0.3	0:00.52 sshd
1832	weblogic	20	0	325m	3476	1120	s	0.0	0.2	0:00.06 watch-smartd
1758	root	20	Û	105m	1912	1548	S	0.0	0.1	0:00.04 bash
1786	weblogic	20	0	105m	1896	1552	s	0.0	0.1	0:00.02 bash
1814	root	20	0	105m	1888	1528	s	0.0	0.1	0:00.01 bash
916	root	20	0	243m	1668	1104	s	0.0	0.1	0:00.04 rsyslogd
1785	root	20	0	141m	1580	1212	S	0.0	0.1	0:00.00 su
948	weblogic	20	0	103m	1540	1228	s	0.0	0.1	0:00.03 startWebLogic.s
934	weblogic	20	0	103m	1536	1228	S	0.0	0.1	0:00.04 startWebLogic.s
1	root	20	0	19232	1508	1240	S	0.0	0.1	0:00.70 init

# 3.2 网络层面排查

在网络层,通过防火墙或相关的入侵防御设备,对 C&C 地址及矿池相关域名/IP 进行监测,涉及域名及 IP 包括:

minergate.com
minexmr.com
78.46.91.134
104.25.208.15
104.25.209.15
136.243.102.167
136.243.102.154
94.130.143.162
88.99.142.163
72 11 140 178

# 附录A WAF 自定义规则防护

针对 WebLogic WLS 组件漏洞的防护过程,WAF 自定义规则的配置可参考如下过程:

1. 新建自定义规则,依次点击"安全管理"-"规则库管理"-"自定义"-"新建"

WAF		安全管理								关于   16 退出
网络层防护	站点防护	自学力策略	自学习结果	规则库管理	策略管理	模板管理	智能补丁	安全交付。	more 👻	2 在线帮助
				2						
规则库管理			自定义							
□ 🔊 通用防	护		Q,条件 ▲							
III We	b插件漏洞		ID							
💷 🖊	以防护		名称							
□ 跨如 □ SQ	4脚本防护 L注入防护		描述							
E LD.	AP注入防护		查询							
🗉 SS	指令防护								1	4.75
II XP	ath注入防护		贝数:0/1 it	录数:0 第一!	丸 上一丸	1 下一页	最末贝		т	新建
·····································	2151主人的护 圣穿越防护		ID	名称		描述			操作	
	建文件包含防护									
□ 内羽	¥过滤						七致活			
💷 We	bShell防护									
	惑信息过滤 #t/T		页数:0/1 订	B录数:0 第一	页 上一页	瓦 下一页	最末页			
	将征 3 = ツ									
<ul> <li>接口状态</li> </ul>	CPU: 49.6 %,	MEM: 35.0 %	圆 许可证有效	文				2017-12-	19 17:21 运行时	间: 21小时 7分钟

2. 将自定义规则命名为"Weblogic wls-wsat RCE"。

新建		×
名称	Weblogic wls-wsat RCE	<b>^</b>
描述信息		- 1
		- 1
告警类型	自定义 🔻	- 1
检测方向	请求 ▼	- 1
设置约束条件	检测对象 URI ▼	
	匹配操作 正则等于 ▼	- 1
	检测值 🕢	- 1
	添加移除	- 1
约束条件		
		-
	确定取消	

- 3. 依次按照如下截图进行设置:
- 检测对象: URI
- 匹配操作:正则包含

### ≫<sup>.</sup>NSFOCUS

#### WebLogic WLS 组件漏洞攻击利用安全预警

#### • 检测值: /wls-wsat/CoordinatorPortType

告警类型	自定义	
检测方向	请求 ▼	
设置约束条件	检测对象URI	¥
	匹配操作	包含 ▼
	检测值 🕜 🛛 /wis-	wsat/CoordinatorPortT
_		添加移除
约束条件	(uri * rco /wls-wsat/Coor	dinatorPortType)

- 检测对象: Request-Body
- 匹配操作:正则包含
- 检测值: (?is)(<object|<new|<method|<void\s+[^>]\*(method|class)\s\*=)

告警类型	自定义	v
检测方向	请求 ▼	
设置约束条件	检测对象	Request-Body v
	匹配操作	正则包含  ▼
	检测值 🕜	\s+[^>]*(method class)\s*=)
		添加移除
约束条件	(uri * rco /wls-wsa ( <object <new <n< td=""><td>at/CoordinatorPortType)&amp;&amp;(request_body * rco (?is) nethod <void\s+[^>]*(method class)\s*=))</void\s+[^></td></object <new <n<>	at/CoordinatorPortType)&&(request_body * rco (?is) nethod  <void\s+[^>]*(method class)\s*=))</void\s+[^>

4. 新建自定义策略,依次点击"安全管理"-"策略管理"-"自定义策略"-"新建"。

## ≫ NSFOCUS

#### WebLogic WLS 组件漏洞攻击利用安全预警

VAF		安全管理									
网络层防护	站点防护	自学习策略	自学习结果	规则库管理	策略管理	模板管理	智能补丁	安全交付 🗸	more 👻		@ 在线
III Web	3 务器/插件防护	1 Î			2						4 新建
🗉 HTTP	访问控制		名称		描述			是否告警	动作	源IP封禁	操作
III Webi	1分 利用防拍										
□ 文件目	1法上传防护					C	无数据				
□ 非法]	「戴限制										
□ 信息流	虚防护										
🗆 🖻 高级防护											
□ 盗链1	沪										
💷 跨站计	家伪造防护										
□ 扫描1	沪										
🗉 Cooki	e安全										
🗉 内容道	t浦										
■ 敏感(	聰过濾										
💷 暴力朝	5解防护										
🔲 XMLI	2击防护										
■ 智能引	擎检测										
□ 🖻 精准防护											
□ 白名单	<u>1</u>										
□ 💕 其他防护											
Ⅲ 例外會	<sup>逻略</sup> 3										
日 自定 日	(策略										

设置策略名称为"Weblogic wls-wsat RCE",勾选刚刚新建的"Weblogic wls-wsat RCE"规则后点击确定。

新建自定义策略	×
基本信息	
名称	Weblogic wls-wsat RCE
	* 名称长度不超过50个字符
描述	
	描述内容不超过200个字符
是否告答	●是◎否
动作	阻断 ▼ ❷
源IP封禁	不封禁  ▼
规则信息	
匹配原则	● 匹配中即结束 ● 匹配中仍继续
Q,规则筛选 ▲	
规则列表	查看 全部 ▼
	GoAhead RCE
	✓ Weblogic wls-wsat RCE
	确定 重置 取消
4	

在站点添加自定义策略,依次点击"安全管理"-"站点防护"-"根据需要选择需要防护的站点"-"Web 安全防护"。

### <sup>≫•</sup>NSFOCUS

#### WebLogic WLS 组件漏洞攻击利用安全预警

WAF	系统监控	安全管理	日志报表	系统管理			1 1 忽	好, admin	简体中文 👻	會升级 鹵	关于 🛛 🖬 退出
网络层防护	站点防护		自学习结果	规则库管理	策略管理	模板管理	智能补丁	安全交付▼	more 👻		0 在线帮助
	9										
站点组	2	+ =	站点组管	慢速攻击防	HTTP Flood 防	数据安全传	Web安全	防例外控	会话追	风险级别控	- 1
🗆 📇 root			理	护	护	榆	4 抽	制	辟	制	
<b>E</b> 192.1	68.21.194		策略模板								
3			模板快速翻	置	选择站点模	板 应用模板	记有配置快速	速配置下列策略	ł		
			协议校验								
				1430	法非法计学校会会			_			
			HIPMAX	10×82	明起出手束呵			•			
			基础防护								- 1
			HTTP访问	控制	请选择策略			•			
			Web服务者	制插件防护	请选择策略			-			
			爬虫防护		请选择策略			-			
			Web通用障	防护	只检测webs	hell策略		•			
			文件非法」		请选择策略			•			
			非法下裁网		请洗择策略			•			
				***	法法保体政						
			15/2/1289	J3₽	用之日千月已和日			•			
			高级防护								
			盗链防护		请选择策略			•			
			跨站请求你	5造防护	请选择策略			•			
● 接□状态 _ 三 (	CPU: 19.2.%	MEM: 34.4 %	@ 许可证有效						2017-12-19	18:14 运行时	■: 21小时 59分轴

7. 在自定义策略中勾选刚刚创建的"Weblgic wls-wsat RCE"策略后,点击确定即可 启用自定义的规则进行防护。

防护效果如下,可以看到,针对该漏洞的攻击已经进行了有效的阻断:

Web安全日志	网络层访问	空制日志 DDoS	防护日志 高危い阻率	日志 Web防蓑波日志 ARP的	始合日志 We	b访问日志 会话追踪日志							
Q.条件 •													
●日期	第目時 合平 ▼ 2017-12-21 12:22 ■ -2017-12-23 12:22 ■												
□事件类型	盘 #20/# -												
- 风险级别			¥	□服务番IP									
□域名	= *			■客户講地理位置 CN, 中回	5	٣							
URI	· · · · · · · · · · · · · · · · · · ·												
同方法	UNRNOWN • BRAAD												
回动作	放过		Ŧ	一百百万百万百万百万万万万万万万万万万万万万万万万万万万万万万万万万万万万万									
	HTTP		Ŧ	○代理信息									
查询													
TT 20-1 /1 - 20-10	(1)	2076 F-1	T_T	土田 海辺新会日本 の									
234.111 23													
本地时间		事件类型	域名	客户编IP	协议类型	URI	风险级别	方法	匹配策略	匹配规则	动作	IP對藥	操作
2017-12-22 11	56:02	自定文攻击	192.168.18.111	192.168.18.120(局域网)	HTTP	/wis%2dwsat/CoordinatorPortTyp	0	POST	Weblgic wis-wsat RCE	Weblogic wis-wsat RCE	咀断	不启用	۲
2017-12-22 11	53:12	自定文攻击	192.168.18.111	192.168.18.120(局域网)	HTTP	/wis%2dwsat/CoordinatorPortTyp	0	POST	Weblgic wis-wsat RCE	Weblogic wis-wsat RCE	阻断	不启用	٠ 🕼

# 附录B NIPS/NIDS 自定义规则防护

部署有绿盟科技 NIPS/NIDS 产品的用户,可参考如下过程自定义防护规则,对 WebLogic WLS 组件远程代码执行漏洞的利用进行阻断和监测。

1. 新建自定义规则,依次点击"对象"-"规则"-"自定义规则"-"新建"。

<sup>™</sup> NSFOCL	JS			WebLo	gic WLS 组	件漏洞攻击	利用安全预警
NIPS					▲ 您好, <u>adm</u>	迎 │ 简体中文 ▼	◎ 关于   ◎ 退出
▶ 首页	系统规则模板	用户规则模板 自定义规则	则例外规则 SQL注入白:	名单 规则查询	>	🕐 在线帮	助 🗖 应用配置
▶ 告警中心	用户能根据		能被用户规则模板引用。				×
▶ 策略							□ 下次不再显示
▼ 对象 <u>1</u>	甘木 喜级						
#UNI 2							4
网络	25 ▼ /凤,共	1余 首页 上一页 1/1 ▼	下一页下页刷新			查找	删除新建
服务	□ 编号	名称			类型	使用	操作
应用	80001	weblogic_wls_ws	sat		TCP		
时间							
敏感数据							
流量通道							
资产树							
▶ 日志报表							
▶ 网络							
・ 系統							

在弹出的窗口中依次进行如下设置:

名称	weblogic_wls_wsat
级别	根据实际需要进行配置
协议类型	TCP
目的端口	Weblogic 服务的端口,默认为 7001
关键字	regex*wls-wsatVCoordinatorPortType.*([ <void <new method <object class]?)+.*< th=""></void <new method <object class]?)+.*<>

### **NSFOCUS**

## WebLogic WLS 组件漏洞攻击利用安全预警

名称 *	weblogic_wls_wsat 规则名称是规则的唯一标识,不可重复命名
级别	◎ 低风险事件 ◎ 中风险事件 ⑧ 高风险事件
匹配范围	● 单包匹配
协议类型	TCP ▼ 以下几项内容不能全部为空
源端口	范围为0~65535
目的端口	7001 范围为0~65535
包长度	范围为0~65535
关键字	regex*wls-wsatVCoordinatorPortType.*([ <void  <new method <object class]?)+.*< th=""></new method <object class]?)+.*<></void  

配置完成后点击右上角"应用配置"。

NIPS						▲ 您好	, <u>admin</u> 简1	本中文 👻 📔 🕴	☞ 关于   ☞ 退出
▶ 首页 ^	系统规则模板	用户规则模板	自定义规则	例外规则	SQL注入白名单	规则查询 >		🕐 在线帮助	🗃 应用配置
▶ 告警中心	用户能根	据持征内容自定义	规则,该规则能被用	1 户规则模材	刻用。				×
▶ 策略									下次不再显示
▼ 对象	甘士 宣祝								
#UQI	<b>垫</b> 4 <b>回</b>	11 4 7 14 7 1			Dier				
网络	25 ▼ /页,	来1余 直页 上-	-凤 1/1 ▼ 下-		用潮			重技	削除新建
服务	□ 编号	名称	:			类型	使用	推	新作
应用	80001	webl	logic_wls_wsat			TCP		E	2
时间									
敏感数据									
流里通道									

2. 新建用户规则模板,依次点击"对象"-"规则"-"用户规则模板"-"新建"。

#### ≫<sup>.</sup>NSFOCUS

### WebLogic WLS 组件漏洞攻击利用安全预警

NIPS			▲應	好, <u>admin</u> )简体中文 <del>▼</del> )	☞ 关于   ┗ 退出
▶ 首页	《 系统规则模板 用」	户规则模板 自定义规则	例外规则 SQL注入白名单	规 > » 🕜 在线帮助	➡ 应用配置
▶ 告警中心	<ol> <li>用户规则模板允许自</li> </ol>	1定义模板,可灵活选择所需	的规则集及其动作。		×
▶ 策略	用户模板规则数量和	11动作都不会随着系统规则库	的升级而更新。	C	] 下次不再显示
					4 新建
<u>网络</u>	名称	备注			操作
服务	weblogic_wls_wsat				2
应用					
时间					
敏感数据					
流里通道					
资产树					
▶ 日志报表					

创建名为"weblogic\_wls\_wsat"的模板,在事件栏中找到刚刚创建的"weblogic\_wls\_wsat" 规则,可根据需求选择规则触发后采取的操作(告警、阻断、隔离、抓包)。

新建					×						
模板名称 * weblogic_wls_wsat											
各注											
四 4上											
♀查询 ▲											
规则名称											
高级选项>>											
查找											
5 ▼ 页,共7935条 首页 上一页 1587/1587 ▼ 下一页 末											
事件	可靠度	□告警	回阻断	隔离②	□抓包						
[67910] HTTP: IIS拒绝服务企图	中										
[70051] TELNET服务TTYPROMPT环境变重内部事件	中										
[70100] Windows SMB Openuser操作	中										
[78999] FTP服务root用户	中										
[80001] weblogic_wls_wsat	中										
5 ▼ 仮,共7935条 首页 上一页 1587/1587 ▼ 下一页 末	5 ▼ /页,共7935条 首页 上一页 1587/1587 ▼ 下一页 末页										
确定	取消										

配置完成后,点击右上角应用配置。

### <sup>≫•</sup>NSFOCUS

## WebLogic WLS 组件漏洞攻击利用安全预警

NIPS			▲ 您好, <u>admin</u> )简体中文 👻	☞ 关于   ┗ 退出
▶ 首页	≪ 系统规则模板	用户规则模板 自定义规则	例外规则 S > » 😢 在线帮助	) 🗏 应用配置
▶ 告警中心	用户规则模板分	许白完义横板,可思话选择所零	的规则使及其动作。	×
▶ 策略	用户模板规则数	里和动作都不会随着系统规则库	的升级而更新。	
▼ 对象				
-				新建
网络	名称	备注		操作
服务	weblogic_wls_wsat			<b>D</b>
应用				
时间				
敏感数据				

3. 创建防护策略,依次点击"策略"-"入侵防护"-"入侵防护策略"-"新建"。

NIPS							▲ 您好, <u>admin</u>			
▶ 首页	入侵	影防护策	略 DoS防护					🕜 在线	帮助	■ 应用配置
▶ 告警中心	3	λ倡防:	的策略用来可罢其	于签名规则的改击	防护, 句公漏洞利用	∃、SOL注入等;				×
▼ 策略 1		系统预	置多种系统规则模	板,基于不同场景	预定义规则范围及其	响应动作。如有	]特殊需求,用户可派生	模板或自定	义用户规	1. 「「「「「「」」 「」」
入侵防护 2										·太小舟亚小 4
数据泄漏防护	25	▼	共1条 首页 上·	─页 1/1 ▼ 下	一页末页		查找	删除	拥	禁用 新建
信誉	gioba	шапу:ң	1 * *							
高级威胁防护		编号	源地址对象	用户	目的地址对象	时间	规则模板	防护模式	使用	操作
URL分类		1	* any	any	i≉ any	any	weblogic_wls_wsat	4	1	🖻 Ӿ 🌒 🗎
防病毒										
用户管理										
应用管理										
流里管理										
▶ 对象									_	

在规则模板中选择刚刚创建的"weblogic\_wls\_wsat"模板。

≫<sup>∙</sup>NSFOCUS

## WebLogic WLS 组件漏洞攻击利用安全预警

新建	×
安全区	global 👻
源地址对象 *	any 👻
目的地址对象 *	any 👻
用户	any 🔻
时间对象 \star	any 👻
规则模板 *	Default -
防护模式	DMZ区服务器
备注	Web服务器 Windows服务器 通用服务器 UNIX类服务器 <u>僵木镭检测</u> weblogic_wls_wsat
	·····································

配置完成后点击右上角"应用配置"。

NIPS				▲ 您好, <u>adn</u>	<u>nin</u>   後	『体中文 ▼    ☞ 关于	-   已 退出				
▶ 首页	入侵防护	入侵防护策略 DoS防护 2 在线帮助 🗏 🖻 🖻									
▶ 告警中心	入侵	防护策略用来配置基于签名规	则的攻击网	, 方护,包含漏洞利用 、SQL	主入等;		×				
▼ 策略	系统预置多种系统规则模板,基于不同场景预定义规则范围及其响应动作。如有特殊需求,用户可派生模板或自定义用户规则模板。										
入最防护						🗌 下次不	項显示				
数据泄漏防护	25 ▼ /页	ī,共 <b>1</b> 条 首页 上一页		查找	删	余   启用   禁用	新建				
信誉	global/any	洪1条 ^									
高级威胁防护	- 编号	, 源地址对象	用户	目的地址对象	时间	规则模板	防护模式				
URL分类		* 001		the opy							
防病毒	1	≁ ally	any	≁ ally	any	weblogic_wis_wsat	×				
用户管理											
应用管理											
流量管理											
→ <sub>对象</sub>	4						÷				

完成上述操作后即可进行防护,防护效果如下,可以看到,针对该漏洞的攻击已经进行 了有效的阻断:

≫ <sup>.</sup> NSFOC	US			WebLogic	WLS 组件漏	同攻击利	利用安全社
NIPS					▲ 您好, <u>admin</u>   简体 <sup>。</sup>	中文 🗸 📔 🛛	☞ 关于   ⊫ 退出
▶ 首页	入侵防护事	件隔离列表			0	在线帮助	🗃 应用配置
′ 告警中心	🗌 自动刷新	10 ▼秒 手i	动刷新				🗌 显示详情
全部	状态	时间	事件	源	目的	认证用户	关联账号
入侵防护事件 数据泄漏事件	A O O	2017-12-22 15:23:14	[80001] weblogic_wls_wsat	192.168.253.1:63856	192.168.253.141:7001		
信誉事件 URI 分类事件	A O O	2017-12-22 15:23:14	[80001] weblogic_wls_wsat	192.168.253.1:63853	192.168.253.141:7001		
防病毒事件							
策略							
対象	•						