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；

一. 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。

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/AdminServ
er/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：

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	TCP
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]?)+.*

效果如下图所示：

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。

```
[root@172-1-2-88 ~]# ls -ls /tmp/
total 2240
   4 drwxr-x--- 2 tomcat   tomcat     4096 Dec 20 02:48 hsperfdata_tomcat
   4 drwxr----- 2 weblogic bea        4096 Dec 20 02:48 hsperfdata_weblogic
2224 -rwxr--r-- 1 weblogic bea     2274080 Dec 19 21:13 watch-smartd
   4 drwxr-x--x 3 root     root       4096 Oct 31 23:47 wlstTemproot
   4 drwxr-x--x 3 weblogic bea        4096 Oct 31 09:31 wlstTempweblogic
[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   0  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

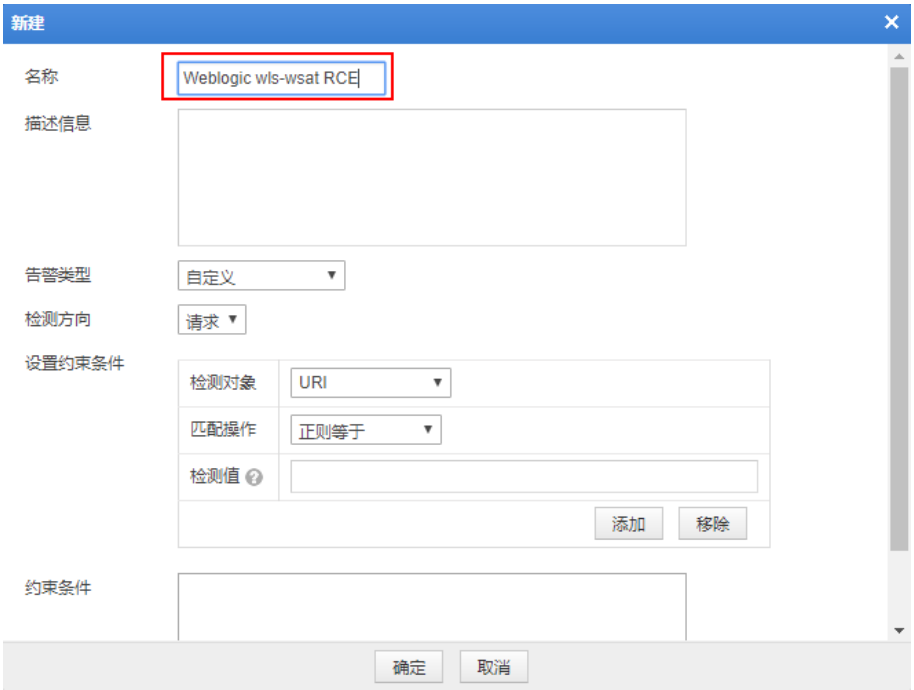
72.11.140.178

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”

2. 将自定义规则命名为“Weblogic wls-wsat RCE”。



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

- 检测值：/wls-wsat/CoordinatorPortType

- 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*=)

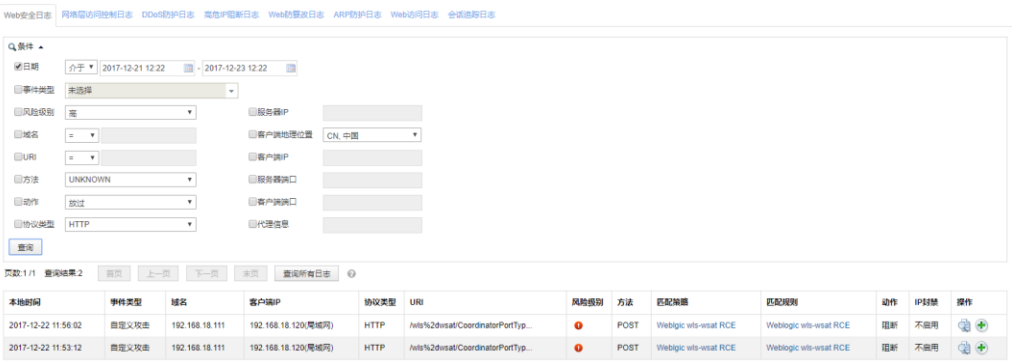
4. 新建自定义策略，依次点击“安全管理”-“策略管理”-“自定义策略”-“新建”。

5. 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。

6. 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”。

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。

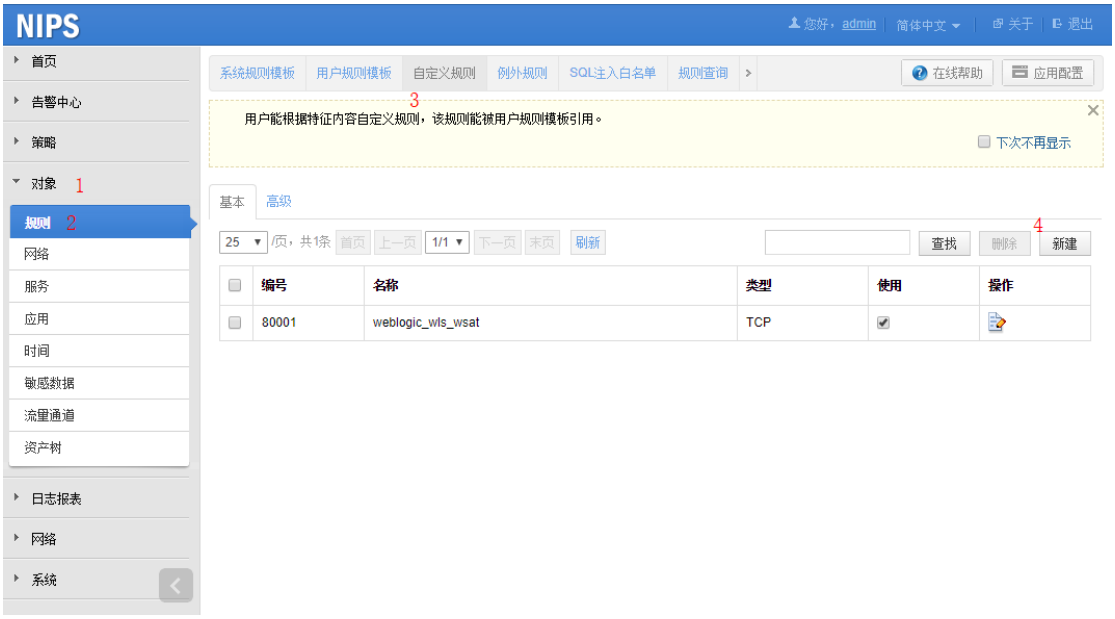
防护效果如下，可以看到，针对该漏洞的攻击已经进行了有效的阻断：



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”。



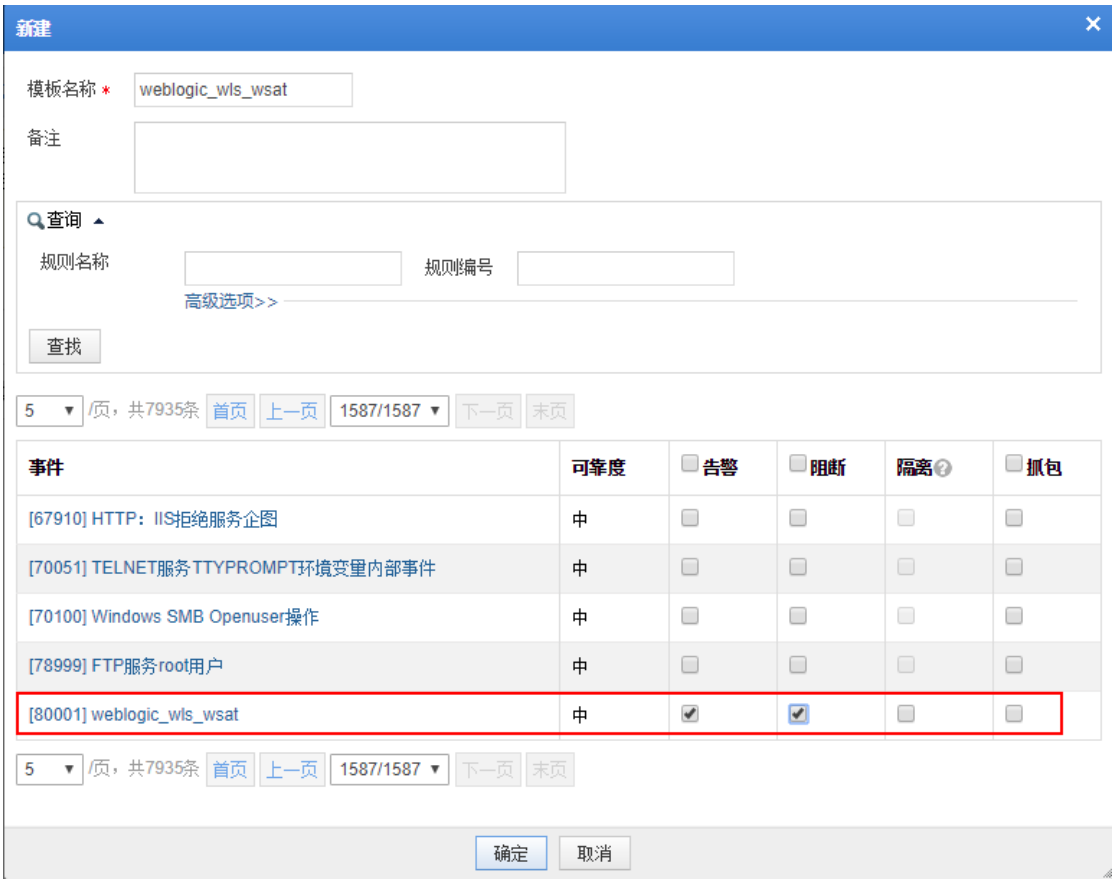
在弹出的窗口中依次进行如下设置：

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-wsat\/CoordinatorPortType.*([<void|<new|method|<object|class]?)+.*

配置完成后点击右上角“应用配置”。

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”。

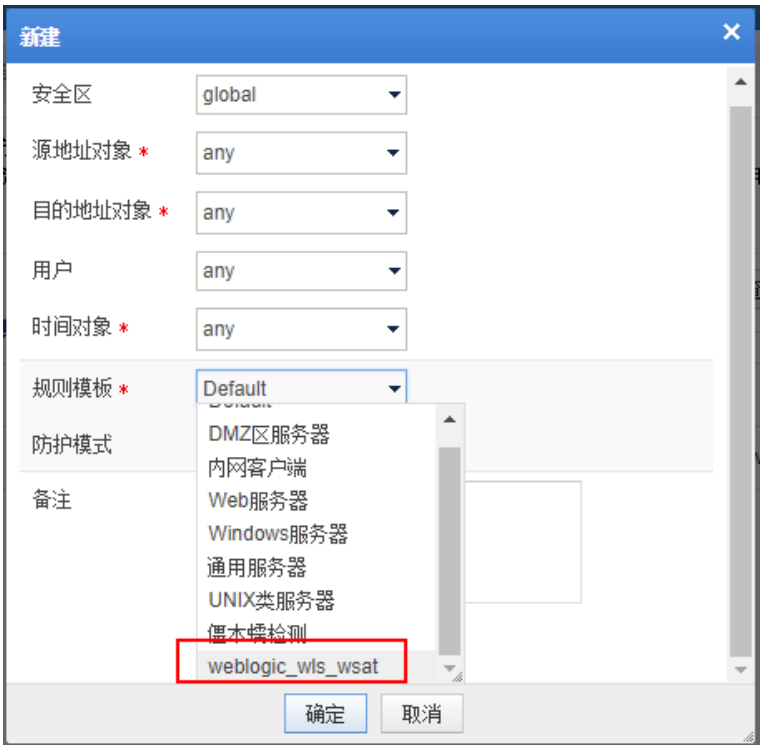
创建名为“weblogic_wls_wsat”的模板，在事件栏中找到刚刚创建的“weblogic_wls_wsat”规则，可根据需求选择规则触发后采取的操作（告警、阻断、隔离、抓包）。



配置完成后，点击右上角应用配置。

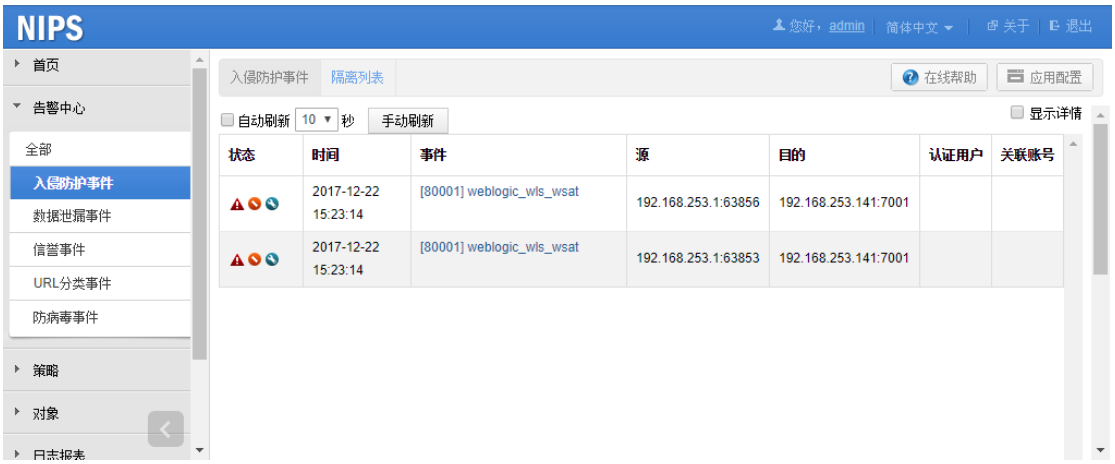
3. 创建防护策略，依次点击“策略”-“入侵防护”-“入侵防护策略”-“新建”。

在规则模板中选择刚刚创建的“weblogic_wls_wsat”模板。



配置完成后点击右上角“应用配置”。

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：


NIPS
您好，admin
简体中文
关于
退出
首页
告警中心
全部
入侵防护事件
数据泄漏事件
信誉事件
URL分类事件
防病毒事件
策略
对象
日志报表
入侵防护事件
隔离列表
在线帮助
应用配置
自动刷新
10
秒
手动刷新
显示详情
状态
时间
事件
源
目的
认证用户
关联账号
2017-12-22 15:23:14
[80001] weblogic_wls_wsat
192.168.253.1:63856
192.168.253.141:7001
2017-12-22 15:23:14
[80001] weblogic_wls_wsat
192.168.253.1:63853
192.168.253.141:7001