Apache Struts2
远程代码执行漏洞（S2-057）
技术分析与防护方案

发布时间：2018 年 8 月 23 日

综述

北京时间 2018 年 8 月 22 日，Apache 官方发布通告公布了 Struts2 中一个远程代码执行漏洞（CVE-2018-11776，CNVD-2018-15894，CNNVD-201808-740）。该漏洞在两种情况下存在，第一，当 xml 配置中未设置 namespace 值，且上层动作配置(action(s) configurations)中未设置或使用通配符 namespace 值时，可能导致远程代码执行漏洞的发生。第二，使用未设置 value 和 action 值的 url 标签，且上层动作配置中未设置或使用通配符 namespace 值，同样可能导致远程代码执行。

相关链接如下：
https://cwiki.apache.org/confluence/display/WW/S2-057

受影响版本

- Struts 2.3 - 2.3.34
- Struts 2.5 - 2.5.16

不受影响版本

- Struts 2.3.35
- Struts 2.5.17

技术防护方案

版本检测

通过配置文件检测

此漏洞产生于低版本的 Struts 组件，当应用系统引入相关组件时，将存在被攻击者远程攻击的风险。建议由应用开发人员排查引入组件的版本是否处于受影响范围之内。

查看 Maven 配置文件 pom.xml 中关于组件的版本。如：

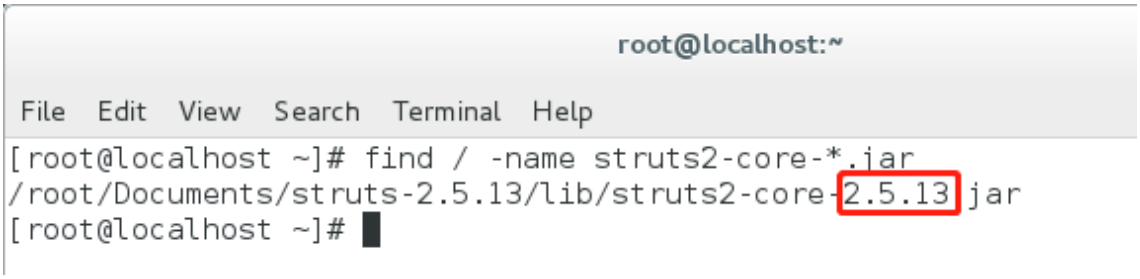
```
<dependency>
    <groupId>org.apache.struts</groupId>
    <artifactId>struts2-core</artifactId>
    <version>2.5.13</version>
</dependency>
```

若红字所示版本在受影响范围内，则请用户尽快升级 Struts2 至最新版本，以保证长期有效的防护。

通过组件名检测

Linux 系统下可使用以下命令查找当前使用的 struts2-core 包，通过查看其文件名，判断当前版本。

```
find / -name struts2-core-*.jar
```



若红框处版本号在受影响范围内，则请用户尽快升级至最新版本。

官方修复方案

官方已在最新版本中修复了此漏洞，请用户尽快将 Struts 升级至官方修复版本，2.3.*的用户请升级至 2.3.35；2.5.*的用户请升级至 2.5.17。下载链接如下所示：

Struts2.3.35:
http://mirrors.hust.edu.cn/apache/struts/2.3.35/struts-2.3.35-all.zip

Struts2.5.17:
http://mirrors.hust.edu.cn/apache/struts/2.5.17/struts-2.5.17-all.zip

临时解决方案

排查所有 Struts 2 的配置文件，如 struts.xml，为没有定义 namespace 命名空间的 package 节点添加命名空间配置。

```
<package name="user" namespace="/user" extends="struts-default">
    <action name="login">
    </action>
</package>
```

绿盟科技防护建议

绿盟科技检测类产品与服务

1、公网资产可使用绿盟云 紧急漏洞在线检测，检测地址如下：
手机端访问地址：
https://cloud.nsfocus.com/megi/holes/hole_struts2_2018_8_23.html
PC 端访问地址：
https://cloud.nsfocus.com/#/krosa/views/initcdr/productandservice?service_id=1026

2、内网资产可以使用绿盟科技的入侵检测系统(IDS)，远程安全评估系统（RSAS V5、V6）和 Web 应用漏洞扫描系统（WVSS）进行检测。

- 入侵检测系统（IDS）
  http://update.nsfocus.com/update/listIds
- 远程安全评估系统（RSAS V5）
  http://update.nsfocus.com/update/listAurora/v/5

- 远程安全评估系统（RSAS V6）
  http://update.nsfocus.com/update/listRsasDetail/v/vulweb
- Web 应用漏洞扫描系统（WVSS）
  http://update.nsfocus.com/update/listWvssDetail/v/6/t/plg

通过上述链接，升级至最新版本即可进行检测！

使用绿盟科技防护类产品进行防护

- 入侵防护系统（IPS）
  http://update.nsfocus.com/update/listIps
- 下一代防火墙系统（NF）
  http://update.nsfocus.com/update/listNf
- Web 应用防护系统（WAF）
  http://update.nsfocus.com/update/wafIndex

通过上述链接，升级至最新版本即可进行防护！

检测防护产品升级包/规则版本号

检测产品	升级包/规则版本号
IDS	5.6.7.732、5.6.8.732、5.6.9.18479、5.6.10.18479
RSAS V5 web 插件包	V051758
RSAS V6 web 插件包	V6.0R02F00.1004
WVSS V6 web 插件包	V6.0R03F00.113

防护产品	升级包/规则版本号
IPS	5.6.7.732、5.6.8.732、5.6.9.18479、5.6.10.18479
NF	5.6.7.732、6.0.1.732
WAF	v6.0.5.1.39591、v6.0.7.0.39590、v6.0.6.1.39589

具体配置详见附录

技术分析

补丁对比

如图所示，补丁主要添加了 cleanNamespaceName 方法，该方法通过白名单的方式来验证 namespace 是否合法，从官方描述和漏洞修复方式来看，该漏洞应该是一个 Ognl 的表达式注入漏洞。

```
        mapping.setNamespace(cleanupNamespaceName(namespace));
        mapping.setName(cleanupActionName(name));
    }

    /**
     * Checks namespace name against allowed pattern if not matched returns default namespace
     *
     * @param rawNamespace name extracted from URI
     * @return safe namespace name
     */
    protected String cleanupNamespaceName(final String rawNamespace) {
        if (allowedNamespaceNames.matcher(rawNamespace).matches()) {
            return rawNamespace;
        } else {
            LOG.warn(
                "{} did not match allowed namespace names {} - default namespace {} will be used!",
                rawNamespace, allowedActionNames, defaultActionName
            );
            return defaultNamespaceName;
        }
    }
```

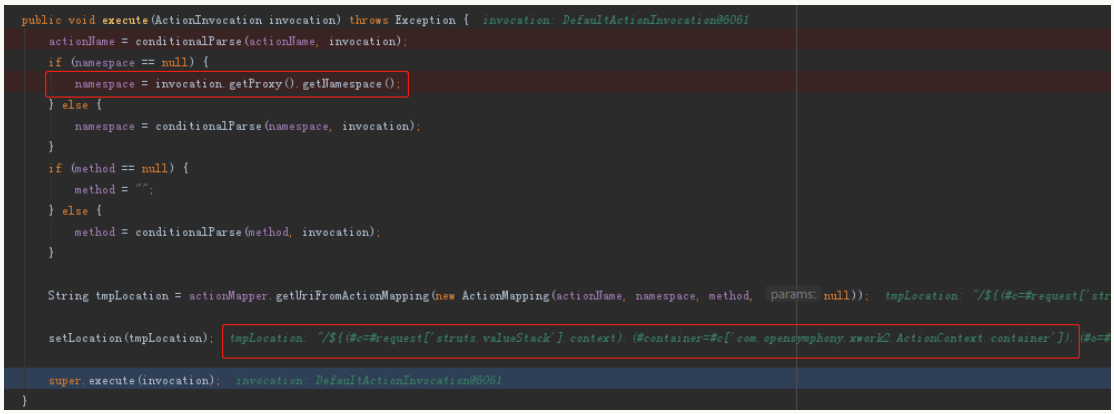
动态分析

漏洞发布几个小时之后，漏洞发现作者公布了整个发现过程，并且详细分析了一种漏洞情形：https://lgtm.com/blog/apache_struts_CVE-2018-11776。按照该博客的说法，拉取 struts2-showcase 项目作为示例，修改 struts-actionchaining.xml，具体如下：

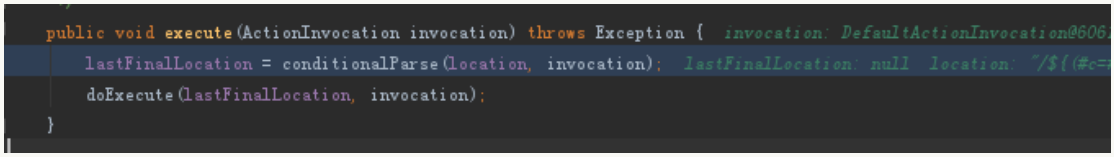
```
<struts>
    <package name="actionchaining" extends="struts-default" >
        <action name="actionChain1" class="org.apache.struts2.showcase.actionchaining.ActionChain1">
            <result type="redirectAction">
                <param name = "actionName">register2</param>
            </result>
        </action>
    </package>
</struts>
```

在这种情况下，所有到 actionChain1.action 的请求的返回结果都会指向 register2，并且执行链会到 ServletActionRedirectResult.execute 方法中，

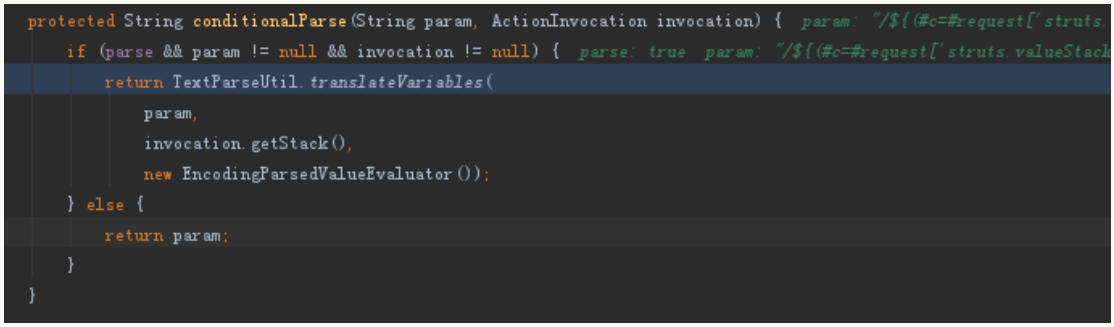
具体如下：



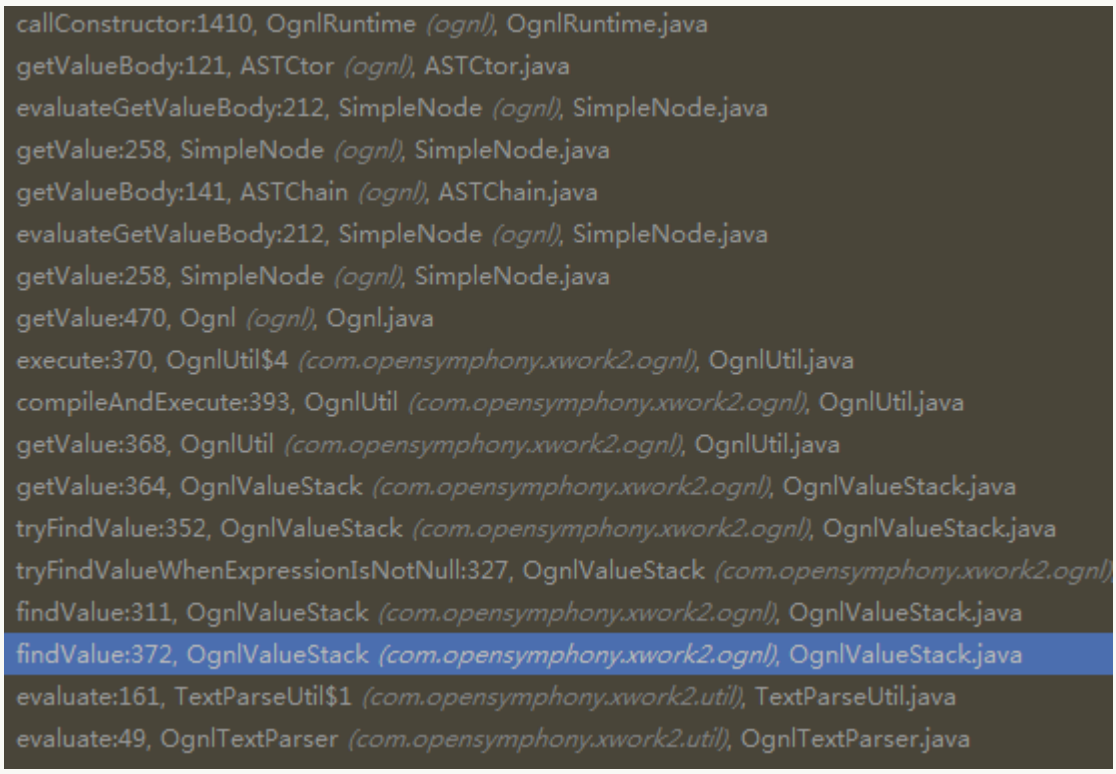
从上图可以看出，通过 namespace 字段，污染了 tmpLocation 字典，并且设置为了预期的执行的 PoC，这也是补丁中为什么要净化 namespace 的原因，继续跟踪 namespace 的去向,执行链会到 ServletActionRedirectResult 的父类的父类 StrutsResultSupport.execute 方法中，具体如下图：



这里有个 conditionParse 方法，这个方式就是使用 Ognl 表达式来计算数据值，在系统中用得非常多，而且在一些历史漏洞中，也应该由它来背锅，当然最大的锅还是 struts 官方，每次漏洞出在哪就修在哪，典型的头痛医头，脚痛医脚。方法实现如下图所示：

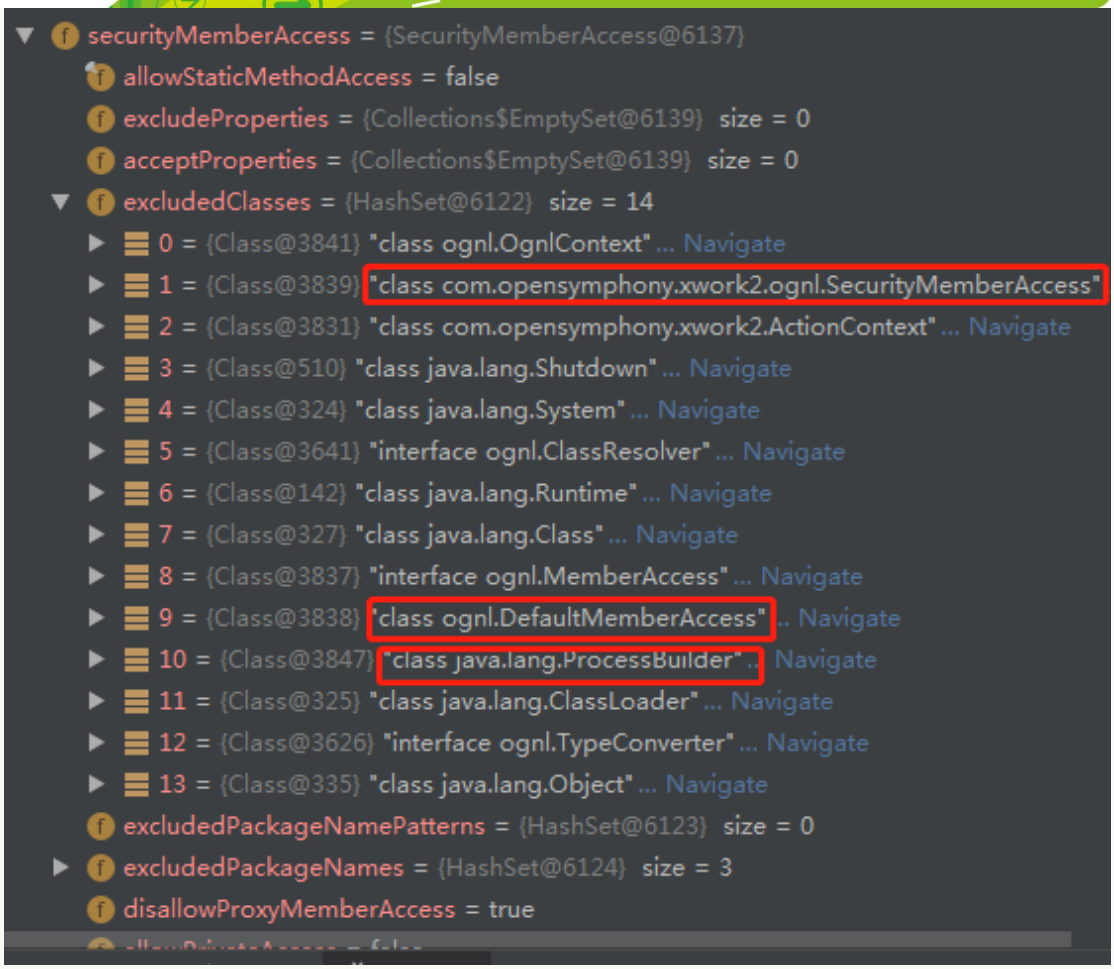


在这个方法中会使用到 TextParseUtil.translateVariables 方法，继续跟踪，调用栈进入 OgnlTextParser 中的 evaluate 方法,首先会判断传入的表达式是否合法，比如是否能找到${}或者%{}对，接着调用 evaluator.evaluate 求值，求值过程非常复杂，总得来说就是链式执行过程，具体如下调用栈：



从上图也可以看出最顶层就是通过反射的方式来调用 ProcessBuilder 的构造函数，中间部分就是链式执行过程中牵涉到一些操作。

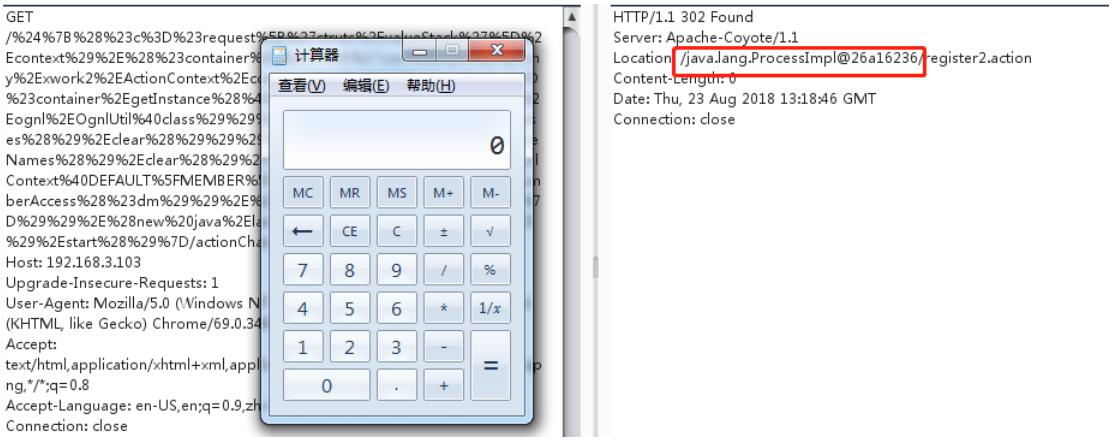
我们可以看下求值过程中参数的一些情况。来查看 Ognl 安全加固的一些变化，具体如下图：



主要是黑名单上又添加了一些类，分别是：

```
class ognl.DefaultMemberAccess
class com.opensymphony.xwork2.ognl.SecurityMemberAccess
class java.lang.ProcessBuilder
```

分析就结束了，计算器还是要弹的，如下图：



附录 产品使用指南

TRG 安全平台提供应急响应手册

TSA（绿盟态势感知平台）

添加“struts2_057 漏洞攻击”事件规则：

进入 BSA 态势感知主页，进入规则引擎 APP，如图 1.1：

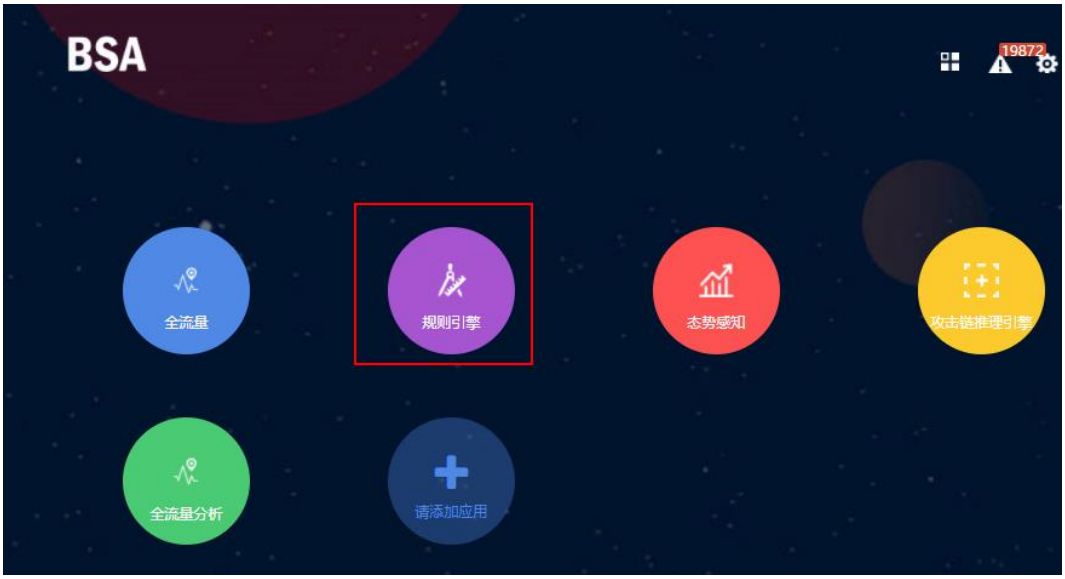


图 1.1 进入规则引擎 APP

1．新建网络入侵规则

新建规则，如图 1.2：

图 1.2 新建规则

在新建页面，如图 1.3：
规则模式：专家模式
规则分类：网络入侵规则
规则 sql：

select sip, dip, sum(last_times) as atk_count, sip, dip, min(timestamp) as start_time, max(timestamp) as end_time, concat_agg(related_id_list) as related_id_list from internal_app_bsaips.ipslog where rule_id =24298
group by sip, dip

图 1.3 新建规则-专家模式填写

点击下一步，出现规则属性设置页面，如图 1.4：
名称：struts_057 漏洞攻击
安全等级：高
事件阶段：攻击渗透
超时时间：1800（默认值）
持续时间：3600（默认值）
归并属性：sip，dip
事件类型：系统入侵事件 - 漏洞攻击
规则描述：该事件是攻击者针对 struts2 漏洞的攻击。
规则建议：如果攻击发起者为我方资产，则说明该资产已失陷。否则，如被攻击系统为我方资产，并且部署有 struts 服务，请确认该资产是否存在事件详情中的漏洞。

图 1.4 新建规则-规则属性设置

点击完成，完成该规则配置。

在规则列表中使之生效，如图 1.5：

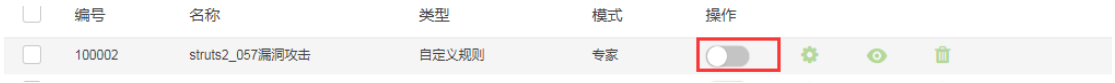


图 1.5 使规则生效

2. 新建网站安全规则

新建规则，如图 1.6：

图 1.6 新建规则

在新建页面，如图 1.7：

规则模式：专家模式

规则分类：网站安全规则

规则 sql：

select sip，dip,LOWER(protocol_type) as protocol_type,LOWER(domain) as domain,dport as dport ,uri as uri ,event_type as event_type_sub,min(timestamp) as start_time,max(timestamp) as end_time,sum(count_num) as atk_count,concat_agg(related_id_list) as related_id_list from internal_app_bsawss.waf_webseclog where rule_id =27004870 group by sip,dip,protocol_type,domain,dport,uri,event_type

图 1.7 新建规则-专家模式填写

点击下一步，出现规则属性设置页面，如图 1.8：

名称：struts_057 漏洞攻击

安全等级：中

事件阶段：攻击渗透

超时时间：1800（默认值）

持续时间：3600（默认值）

归并属性：sip,dip,protocol_type,domain,dport,uri

事件类型：系统入侵事件 - 漏洞攻击

规则描述：该事件是攻击者针对 struts2 漏洞的攻击。

规则建议：如果攻击发起者为我方资产，则说明该资产已失陷。否则，如被攻击系统为我方资产，并且部署有 struts 服务，请确认该资产是否存在事件详情中的漏洞。

图 1.8 新建规则-规则属性设置

点击完成，完成该规则配置。

在规则列表中使之生效，如图 1.9.

图 1.9 使规则生效

ESP（绿盟企业安全平台）

更新“Apache struts2 漏洞利用”事件规则：

打开 ESP 绿盟企业安全平台，进入 安全分析 -> 事件规则，查询找到 Apache struts2 漏洞利用，如图 2.1 所示，点击编辑按钮。

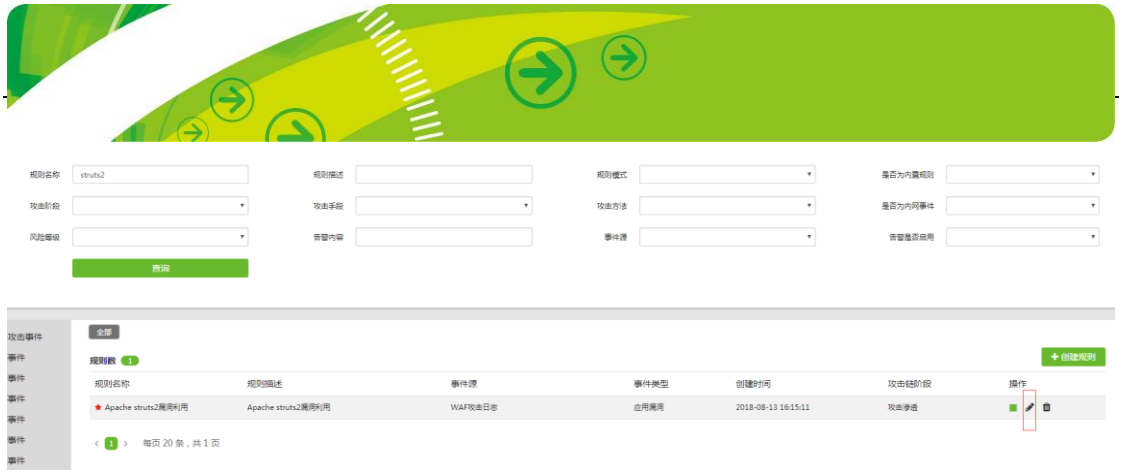


图 2.1 选择编辑规则

点击规则配置中设置，如图 2.2：

图 2.2 点击设置

如下图 2.3，追加 id 到最后 27004870，点击确定：

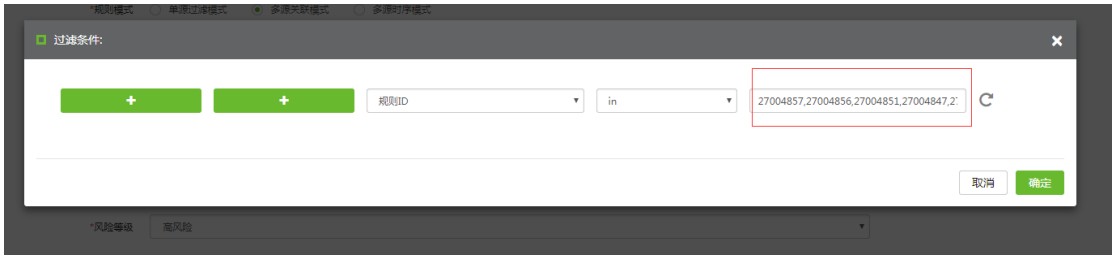


图 2.3 规则设置

点击完成规则创建，效果如图 2.4。

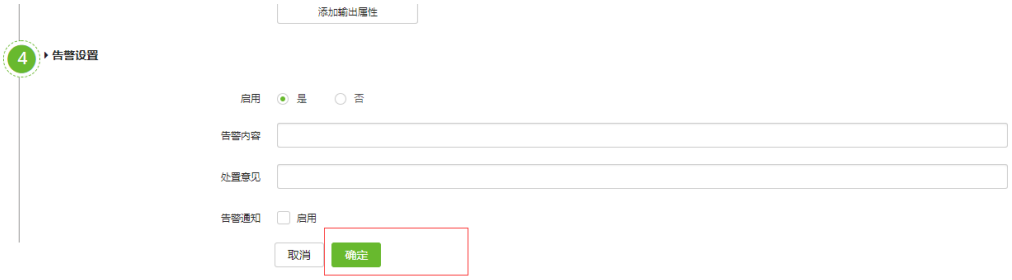


图 2.4 点击完成

1. 编辑“Apache struts2 漏洞攻击事件”事件规则

说明：如果 UTS 已经升级，则可以直接修改“Apache struts2 漏洞攻击事件”规则节点内容，使其包含 UTS 最新的 Struts2-057 设备规则。

1）进入全流量事件规则配置文件文件目录(/home/bsauser/BSA/apps/bsa_tam2/conf)，备份 mergeconf.xml 文件，然后利用 vi 打开 mergeconf.xml 文件，如图 3.1。

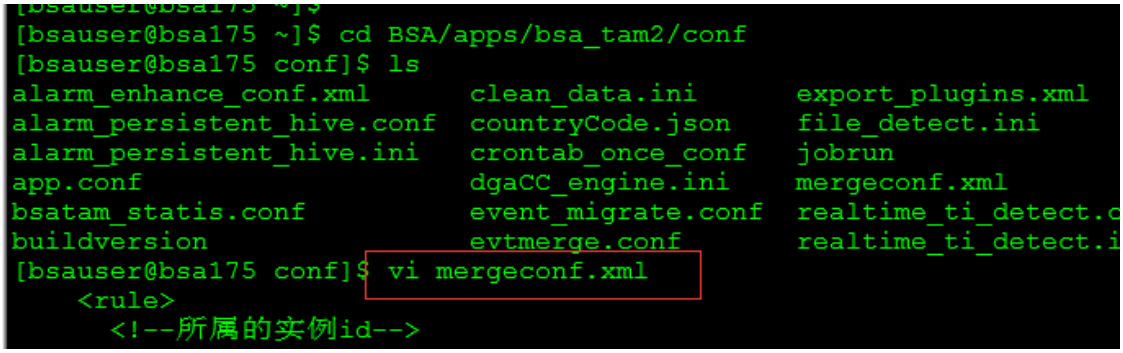


图 3.1 打开全流量事件规则配置文件

2）使用/Struts2 找到“Apache struts2 漏洞攻击事件”规则节点，在 sql 的 rule_id in 内容的括号内增加 24298，并保存退出，规则自动生效。

图 3.2 修改“Apache struts2 漏洞攻击事件”规则节点

2. 新建自定义场景

说明：如果 UTS 并未升级，或者期望回溯之前的 Struts2-057 利用情况，可以使用全流量的自定义场景功能。

1）从 BSA 平台进入全流量分析 APP 选择“场景管理”>“场景配置”>“自

定义场景”>“新建”，步骤如图 3.3-3.6。

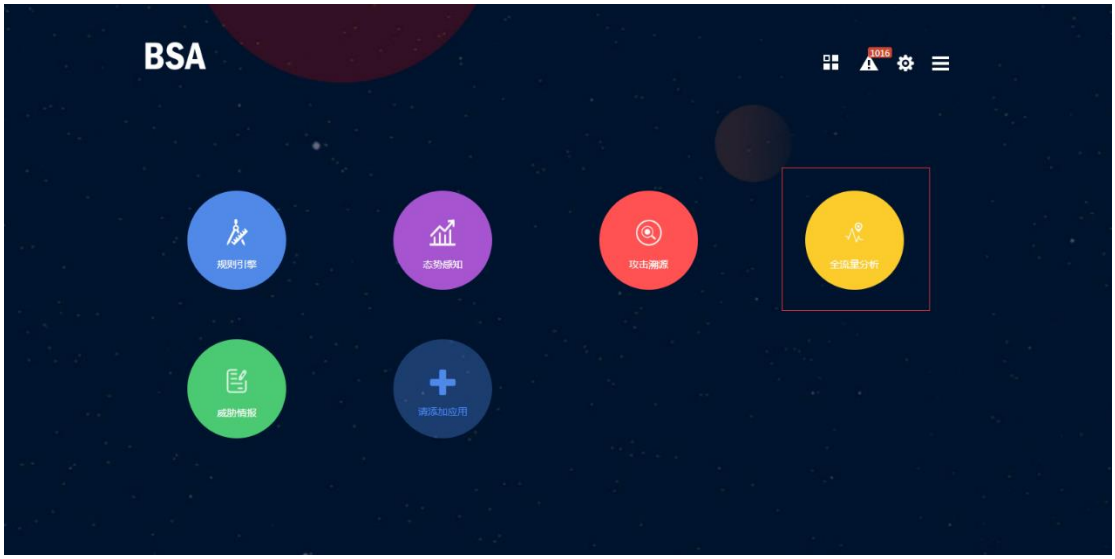


图 3.3 打开 BSA 平台

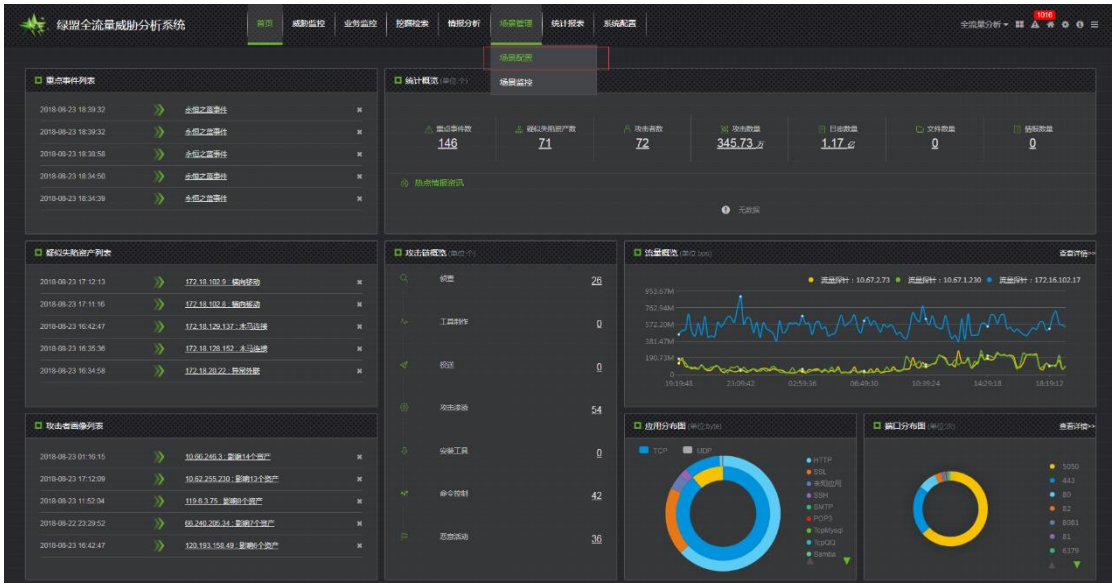


图 3.4 打开全流量分析 APP

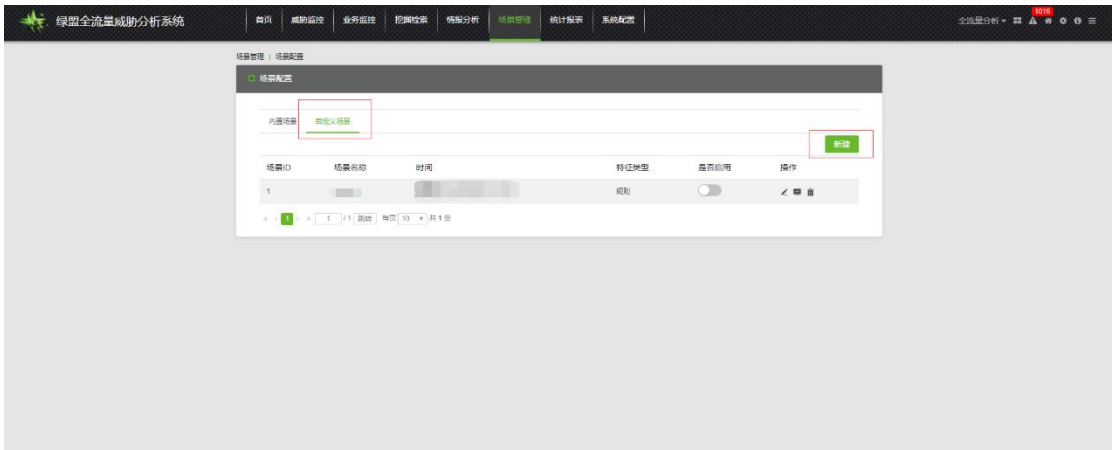


图 3.5 打开场景管理的场景配置

2）在编辑页面增加如下内容，其中回溯数据范围和回溯开始时间，可配置，最后点击确定生成时间。Sql 为：

```
select sip,dip,-1 as sport,dport,min(timestamp) as start_time,max(timestamp) as end_time,first_value(sip_int) as sipv4_int,first_value(srccountryname) as src_country,first_value(srcsubdivisionname) as src_province,first_value(srccityname) as src_city,first_value(dip_int) as dipv4_int,first_value(dstcountryname) as dst_country,first_value(dstsubdivisionname) as dst_province,first_value(dstcityname) as dst_city from internal_app_bsatam2.tam_httplog where method='GET' and (uri like '%java.lang.Runtime%' or uri like '%java.lang.ProcessBuilder%') group by sip,dip,dport
```

细节配置情况如图 3.6 所示：

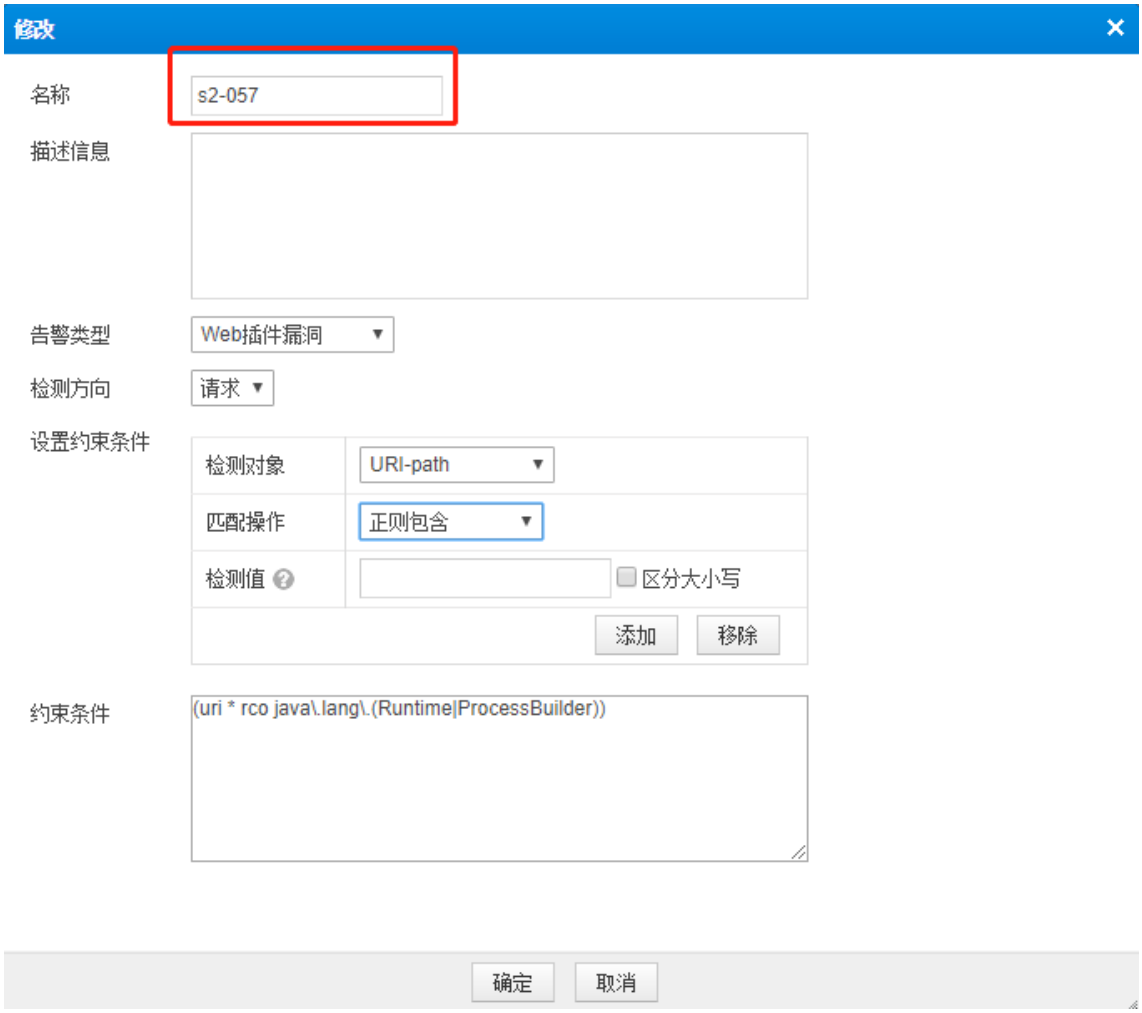
图 3.6 增加自定义场景

WAF 自定义规则配置

请参考如下步骤对临时规则进行部署：

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“s2-057”。

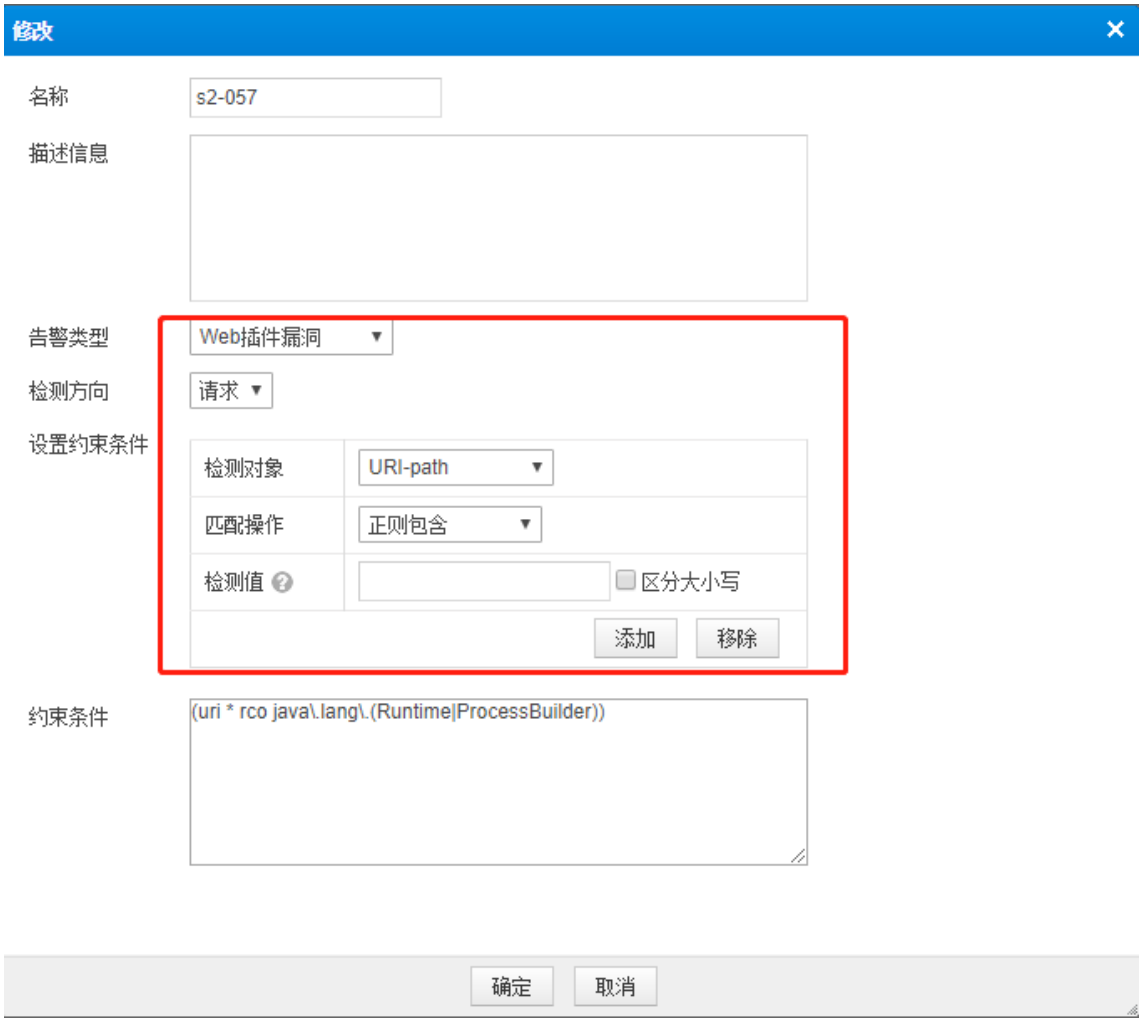


3. 依次按照如下截图进行设置：

检测对象：URI-path

匹配操作：正则包含

检测值：java\.lang\.(Runtime|ProcessBuilder)



配置完成后可以看到如下约束条件：

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”。

设置策略名称为“s2-057 策略”，勾选刚刚新建的“s2-057”规则后点击确定。

5. 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”。

在自定义策略中勾选刚刚创建的“s2-057 策略”后，点击确定即可启用自定义的规则进行防护。

WAF 防护配置

从官网下载对应的规则升级包：
http://update.nsfocus.com/update/downloads/id/22273

WEB应用防护系统(WAF) 规则 6.0.7.0升级包列表

名称： update_rule.v6.0.7.0.39590.wcl	**版本：** v6.0.7.0.39590
MD5： 81269ef8b21af3462d4cef137e24869c	**大小：** 2.07M

描述：

一、新增规则

1.服务器/插件漏洞防护

27004870 struts2_s2_057_rce 防护Struts2 s2-057远程代码执行漏洞

二、修改规则

无

三、删除规则

无

四、升级建议

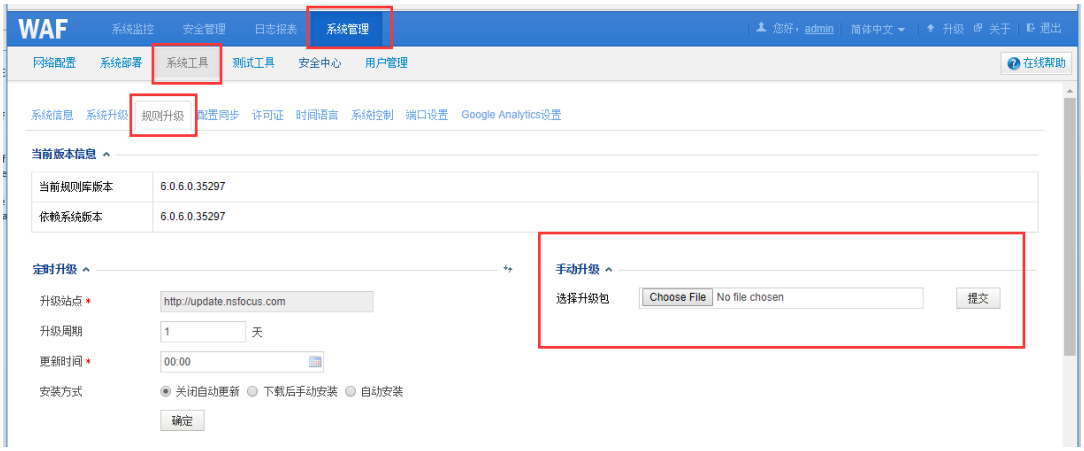
(1) 请在64位系统版本6.0.7.0.39230及以上版本进行升级。

(2) 升级后无需重启设备和引擎。

(3) 如果要应用规则，请为防护站点勾选对应的规则。

发布时间： 2018-08-23 17:43:06

在 WAF 的规则升级界面进行升级：



手动选择规则包，点击提交后即可升级成功。

NIPS 防护配置指导

已经部署绿盟网络入侵防护系统（NIPS）的用户，可通过规则升级进行有效的防护，请相关用户可参考以下步骤进行规则库升级。

1. 从官网下载最新的 NIPS 升级包，以 5.6.10 版本为例，访问以下链接可获得最新的规则升级包：

http://update.nsfocus.com/update/downloads/id/22260

网络入侵防护系统(IPS)规则5.6.10升级包列表

名称：eoi.unify.allrulepatch.ips.5.6.10.18479.rule	版本：5.6.10.18479
MD5：34496185ed375c18a5b2f6f4356945f4	大小：22.48M

描述：

本升级包为入侵防护特征库升级包，仅支持在固件版本5.6R10F00之上，引擎版本5.6R10F00及以上升级。升级包为全量升级包。升级后固件版本和引擎版本不变，规则版本变为5.6.10.18479。该升级包新增/改进的规则有:

新增规则:

1. 攻击[24296]:Adobe Acrobat EMF EmfPlusDrawLines计数堆缓冲区溢出漏洞(CVE-2018-5067)
2. 攻击[24297]:Node.js nghttp2 nghttp2_frame_altsvc_free 空指针引用(CVE-2018-1000168)
3. 攻击[24298]:Struts2远程命令执行漏洞(CVE-2018-11776)(S2-057)

更新规则:

1. 攻击[24294]:Apache Solr XML 外部实体注入漏洞(CVE-2018-8010,CVE-2018-8026)

注意事项:

1. 该升级包升级后引擎自动重启生效，不会造成会话中断，但ping包会丢3~5个，请选择合适的时间升级.

NSFOCUS NIDS/NIPS product signature upgrade package, depends on firmware version at least 5.6R10F00 and engine version 5.6R10F00. This is a total upgrade package. After upgrade package is imported, firemare version and engine version willnot change, signature version will change to 5.6.10.18479. This package include changed rules:

new rules:

1. threat[24296]:Adobe Acrobat EMF EmfPlusDrawLines Count Heap Buffer Overflow Vulnerability(CVE-2018-5067)
2. threat[24297]:Node.js Foundation Node.js nghttp2 nghttp2_frame_altsvc_free Null Pointer Dereference(CVE-2018-1000168)
3. threat[24298]:Struts2 Remote Command Execution Vulnerability(CVE-2018-11776)(S2-057)

update rules:

1. threat[24294]:Apache Solr ConfigSets XML External Entity Expansion Information Disclosure(CVE-2018-8010,CVE-2018-8026)

Announcements:

1. After update the package, the engine will restart automatically, this will don't interrupt sessions, but will cause 3-5 packets loss on ping opereate", please update on a suitable time.

发布时间：2018-08-23 18:24:08

2. 在系统升级中点击离线升级，选择系统规则库，选择对应的文件，点击上传。

3. 更新成功后，在系统默认规则库中查找规则编号：24298，即可查询到对应的规则详情。

注意事项：该升级包升级后引擎自动重启生效，不会造成会话中断，但 ping 包会丢 3~5 个，请选择合适的时间升级。

NF 防护配置指导

绿盟下一代防火墙系统（NF）即将发布针对此漏洞的防护规则，请相关用户及时关注官网规则发布平台，第一时间进行规则升级，访问链接如下：

http://update.nsfocus.com/update/listNewNfDetail/v/rule6.0.1

规则升级可参考以下步骤：

1. 从官网下载最新的 NF 升级包，以 6.0.1 版本为例，访问以下链接可获得最新的规则升级包：

http://update.nsfocus.com/update/listNewNfDetail/v/rule6.0.1

2. 在 NF 的规则升级界面进行升级：

3. 手动选择规则包，点击提交即可完成更新。

RSAS 扫描配置

请相关用户访问以下链接，下载并升级到最新插件版本，RSAS 可提供针对此漏洞的扫描能力。

以 RSAS 6.0 版本为例，访问以下链接可下载针对 s2-057 的规则包：

http://update.nsfocus.com/update/downloads/id/22281

远程安全评估系统（RSAS6.0）Web插件升级包列表

如果要安装多个升级包，请按照日期先后顺序安装；灰色的升级包无需安装。

名称： rsas-vulweb-V6.0R02F00.1004.dat	**版本：** V6.0R02F00.1004
MD5： 05242b5e3f8a98a59e0d505849d96401	**大小：** 408.3K

描述：

本升级包为web插件升级包，支持的web插件版本为V6.0R02F00.1003。升级包为增量升级包，升级后系统版本不变，web插件版本变更为V6.0R02F00.1004。

该升级包包含的变动有：

1. 增加Apache Struts2 S2-057 远程代码执行漏洞（CVE-2018-11776）扫描插件。

注意事项：

1. 本升级包升级完成后自动重启引擎生效，升级过程中可能会影响正在使用的功能，请选择在合适的时间进行升级。

发布时间： 2018-08-23 19:00:34

在系统升级中，点击下图红框位置选择文件。

选择下载好的相应升级包，点击升级按钮进行手动升级。等待升级完成后，可通过定制扫描模板，针对此漏洞进行扫描。

声　明

本安全公告仅用来描述可能存在的安全问题，绿盟科技不为此安全公告提供任何保证或承诺。由于传播、利用此安全公告所提供的信息而造成的任何直接或者间接的后果及损失，均由使用者本人负责，绿盟科技以及安全公告作者不为此承担任何责任。绿盟科技拥有对此安全公告的修改和解释权。如欲转载或传播此安全公告，必须保证此安全公告的完整性，包括版权声明等全部内容。未经绿盟科技允许，不得任意修改或者增减此安全公告内容，不得以任何方式将其用于商业目的。

关于绿盟科技

北京神州绿盟信息安全科技股份有限公司（简称绿盟科技）成立于 2000 年 4 月，总部位于北京。在国内外设有 30 多个分支机构，为政府、运营商、金融、能源、互联网以及教育、医疗等行业用户，提供具有核心竞争力的安全产品及解决方案，帮助客户实现业务的安全顺畅运行。

基于多年的安全攻防研究，绿盟科技在网络及终端安全、互联网基础安全、合规及安全管理等领域，为客户提供入侵检测/防护、抗拒绝服务攻击、远程安全评估以及 Web 安全防护等产品以及专业安全服务。

北京神州绿盟信息安全科技股份有限公司于 2014 年 1 月 29 日起在深圳证券交易所创业板上市交易，股票简称：绿盟科技，股票代码：300369。

绿盟科技官方微博二维码

绿盟科技官方微信二维码