Java反序列化备忘录

phorse / 2018-02-08 13:49:59 / 浏览数 14145 安全技术 资源分享 顶(3) 踩(0)

注：此备忘录翻译自Java-Deserialization-Cheat-Sheet

Java反序列化备忘录

一个为渗透工程师和安全研究人员准备的Java反序列化漏洞备忘录。
阅读需知：

1. 科学上网
2. "被黑掉的应用"栏下是漏洞产生的条件要求

Java Native Serialization (binary)

概述

- 常见问题
- 转载自FoxGlove安全团队的原理介绍

有关大会的PPT和文档

《Marshalling Pickles》

演讲者：@frohoff & @gebl

- 视频
- PPT
- 其余材料

《利用Java中的反序列化漏洞》

演讲者：@matthias_kaiser

- 视频

连环杀手：寂静的Java反序列化渗透

演讲者：@pwntester & @cschneider4711

- PPT
- 白皮书
- 绕过技巧锦集

《我如何开始学会并担忧Java反序列化漏洞》

演讲者：@frohoff & @gebl

- PPT

幸存的Java序列化启示

演讲者：@cschneider4711 & @pwntester

- PPT
- 视频
- 针对Scala, Groovy库的PoC

Java反序列化漏洞 - 被遗忘的Bug类

演讲者：@matthias_kaiser

- PPT

反序列化漏洞引发的信息泄露

演讲者：@matthias_kaiser

- PPT
- 白皮书
- jms利用工具

如何防范Java反序列化漏洞

演讲者：@lucacarettoni

- PPT

从JNDI / LDAP操作到远程执行代码

演讲者：@pwntester and O. Mirosh

- PPT
- 白皮书

如何修复Java序列化紊乱

演讲者：@e_rnst

- PPT+Source

盲打Java反序列化漏洞

演讲者：deadcode.me

- Part I - 常见利用方式
- Part II - 进阶利用

Java虚拟机（JVM）中的反序列化漏洞概述

演讲者：@joaomatosf

- PPT
- 示例

有效攻击载荷生成器

ysoserial

https://github.com/frohoff/ysoserial

其它工具:

- JavaSerialKiller
- Java Deserialization Scanner
- Burp-ysoserial
- SuperSerial
- SuperSerial-Active

如何植入shell(pipes, redirects and other stuff):

- $@|sh – Or: Getting a shell environment from Runtime.exec
- Set String[] for Runtime.exec (patch ysoserial's payloads)
- Shell Commands Converter

攻击原理

- https://blog.srcclr.com/commons-collections-deserialization-vulnerability-research-findings/
- http://gursevkalra.blogspot.ro/2016/01/ysoserial-commonscollections1-exploit.html

JRE8u20_RCE_Gadget

https://github.com/pwntester/JRE8u20_RCE_Gadget

纯粹的JRE 8 RCE反序列化小工具

ACEDcup

https://github.com/GrrrDog/ACEDcup

文件上传通过：

- Apache Commons FileUpload <= 1.3 (CVE-2013-2186) and Oracle JDK < 7u40

Universal billion-laughs DoS

https://gist.github.com/coekie/a27cc406fc9f3dc7a70d

使用默认的Java类（JRE）仍会导致Dos攻击

Universal Heap使用阵列和HashMaps溢出DoS

https://github.com/topolik/ois-dos/

如何运行:

- Java Deserialization DoS - payloads

使用默认的Java类（JRE）仍会导致Dos攻击

Exp工具

工具无特定规范 - 并不需要一个特殊的工具 (就用Burp/ZAP + 有效攻击载荷就OK)

RMI

- 协议
- 默认端口 - 1099/tcp for rmiregistry

ysoserial (仅针对RMI注册表服务)

JMX

- 基于RMI协议
  - CVE-2016-3427
- 在新版本的JRE中部分修补

ysoserial

JexBoss

JNDI/LDAP

- 当我们控制一个地址来查找JNDI（context.lookup（address））并且可以从服务器上反向连接。
- 详细
- JNDI 远程代码执行

https://github.com/zerothoughts/jndipoc

JMS

- 详细

JMET

JSF ViewState

- Mac地址检测不完善

没有专门的工具

JexBoss

T3 of Oracle Weblogic

- Protocol
- Default - 7001/tcp on localhost interface
- CVE-2015-4852
- Blacklist bypass

loubia (在11g和12c上测试, 支持 t3s)

JavaUnserializeExploits (不适用于所有Weblogic版本)

WLT3Serial

IBM Websphere (1)

- 需要是admin身份
- 默认端口 - 8880/tcp
- CVE-2015-7450

JavaUnserializeExploits

serialator

IBM Websphere (2)

- 要求能够使用自定义表单身份验证
- WASPostParam cookie
- 详细

没有专门的工具

Red Hat 系统下的JBoss (1)

- http://jboss_server/invoker/JMXInvokerServlet
- 默认端口 - 8080/tcp
- CVE-2015-7501

JavaUnserializeExploits

https://github.com/njfox/Java-Deserialization-Exploit

serialator

JexBoss

Red Hat JBoss 6.X

- http://jboss_server/invoker/readonly
- 默认端口 - 8080/tcp
- CVE-2017-12149
- JBoss 6.X and EAP 5.X
- Details

没有专门的工具

Red Hat JBoss 4.x

- http://jboss_server/jbossmq-httpil/HTTPServerILServlet/
- <= 4.x
- CVE-2017-7504

没有专门的工具

Jenkins (1)

- Jenkins CLI
- 默认端口 - 高位tcp端口
- CVE-2015-8103
- CVE-2015-3253

JavaUnserializeExploits

JexBoss

Jenkins (2)

- 补丁绕过 Jenkins
- CVE-2016-0788
- 利用复现

ysoserial

Jenkins (s)

- Jenkins CLI LDAP
- *默认端口 - 高位TCP端口
- <= 2.32
- <= 2.19.3 (LTS)
- CVE-2016-9299

Metasploit有针对CVE-2016-9299的攻击模块

CloudBees Jenkins

- <= 2.32.1
- CVE-2017-1000353
- Details

Sploit

Restlet

- <= 2.1.2
- Rest API接受序列化对象时 (使用 ObjectRepresentation)

没有专门的工具

RESTEasy

- 当Rest API接受序列化对象 (uses @Consumes({"\/*"}) or "application/*")
- 详细信息和示例

没有专门的工具

OpenNMS

- RMI

ysoserial

Progress OpenEdge RDBMS

- 全版本
- RMI

ysoserial

Commvault Edge Server

- CVE-2015-7253
- cookie中的序列化数据

没有专门的工具

Symantec Endpoint Protection Manager

- /servlet/ConsoleServlet?ActionType=SendStatPing
- CVE-2015-6555

serialator

Oracle MySQL 企业级监视器

- https://[target]:18443/v3/dataflow/0/0
- CVE-2016-3461

没有专门的工具

serialator

PowerFolder 商业级中间件

- 自定义(?) 协议 (1337/tcp)
- MSA-2016-01

powerfolder-exploit-poc

Solarwinds 虚拟代理

- <= 6.3.1
- RMI
- CVE-2016-3642

ysoserial

思科Prime基础设施

- https://[目标URL]/xmp_data_handler_service/xmpDataOperationRequestServlet
- <= 2.2.3 Update 4
- <= 3.0.2
- CVE-2016-1291

CoalfireLabs/java_deserialization_exploits

Cisco ACS

- <= 5.8.0.32.2
- RMI (2020 tcp)
- CSCux34781

ysoserial

Apache XML-RPC

- all version, no fix (the project is not supported)
- POST XML request with ex:serializable element
- 详细信息和示例

没有专门的工具

Apache Archiva

- 因使用 Apache XML-RPC而产生
- CVE-2016-5004
- 详细信息和示例

没有专门的工具

SAP NetWeaver

- https://[target]/developmentserver/metadatauploader
- CVE-2017-9844

PoC

Sun Java Web Console

- 用于Solaris的管理员面板
- < v3.1.
- old DoS sploit

没有专门的工具

Apache MyFaces Trinidad

- 1.0.0 <= version < 1.0.13
- 1.2.1 <= version < 1.2.14
- 2.0.0 <= version < 2.0.1
- 2.1.0 <= version < 2.1.1
- 未设定检查MAC地址
- CVE-2016-5004

没有专门的工具

Apache Tomcat JMX

- JMX
- 补丁绕过
- CVE-2016-8735

JexBoss

OpenText Documentum D2

- version 4.x
- CVE-2017-5586

利用

Liferay

- /api/spring
- /api/liferay
- <= 7.0-ga3
- IP检查不完善
- Details

没有专门的工具

Apache ActiveMQ - Client lib

- JMS

JMET

Redhat/Apache HornetQ - Client lib

- JMS

JMET

Oracle OpenMQ - Client lib

- JMS

JMET

IBM WebSphereMQ - Client lib

- JMS

JMET

Oracle Weblogic - Client lib

- JMS

JMET

Pivotal RabbitMQ - Client lib

- JMS

JMET

IBM MessageSight - Client lib

- JMS

JMET

IIT Software SwiftMQ - Client lib

- JMS

JMET

Apache ActiveMQ Artemis - Client lib

- JMS

JMET

Apache QPID JMS - Client lib

- JMS

JMET

Apache QPID - Client lib

- JMS

JMET

Amazon SQS Java Messaging - Client lib

- JMS

JMET

检测

代码审计

- ObjectInputStream.readObject
- ObjectInputStream.readUnshared
- Tool: Find Security Bugs
- Tool: Serianalyzer

数据交互

- 序列化数据标识符--'ac ed 00 05'（十六进制）
- 序列化数据标识符--'rO0'（Base64编码下）
- 请求包的Content-Type header为'application/x-java-serialized-object'

网络

- Nmap >=7.10 有很多Java相关漏洞的探针
- 使用nmap --all-version 命令在非标准端口上查找JMX / RMI

Burp 插件

- JavaSerialKiller
- Java Deserialization Scanner
- Burp-ysoserial
- SuperSerial
- SuperSerial-Active

被黑掉的应用 (without public sploits/need more info)

Spring服务调用 (HTTP, JMS, RMI...)

- 细节

SAP P4

- info from PPT

Apache SOLR

- SOLR-8262
- 5.1 <= version <=5.4
- 流处理程序使用RPC的Java序列化

Apache Shiro

- SHIRO-550
- 加密的cookie（使用硬编码密钥）

Apache ActiveMQ (2)

- CVE-2015-5254
- <= 5.12.1
- 漏洞信息
- CVE-2015-7253

Atlassian Bamboo (1)

- CVE-2015-6576
- 2.2 <= version < 5.8.5
- 5.9.0 <= version < 5.9.7

Atlassian Bamboo (2)

- CVE-2015-8360
- 2.3.1 <= version < 5.9.9
- Bamboo JMS port (port 54663)

Atlassian Jira

- only Jira with a Data Center license
- RMI (port 40001)
- JRA-46203

Akka

- version < 2.4.17
- "可通过Akka远程TCP连接的ActorSystem"
- Official description

Spring AMPQ

- CVE-2016-2173
- 1.0.0 <= version < 1.5.5

Apache Tika

- CVE-2016-6809
- 1.6 <= version < 1.14
- Apache Tika的MATLAB解析器

Apache HBase

- HBASE-14799

Apache Camel

- CVE-2015-5348

Apache Log4j

- 作为服务器
- CVE-2017-5645

Gradle (gui)

- custom(?) protocol(60024/tcp)
- article

Oracle Hyperion

- from PPT

Oracle Application Testing Suite

- CVE-2015-7501

Red Hat JBoss BPM Suite

- RHSA-2016-0539
- CVE-2016-2510

VMWare vRealize Operations

- 6.0 <= version < 6.4.0
- REST API
- VMSA-2016-0020
- CVE-2016-7462

VMWare vCenter/vRealize (various)

- CVE-2015-6934
- VMSA-2016-0005
- JMX

Cisco (various)

- List of vulnerable products
- CVE-2015-6420

Lexmark Markvision Enterprise

- CVE-2016-1487

McAfee ePolicy Orchestrator

- CVE-2015-8765

HP iMC

- CVE-2016-4372

HP Operations Orchestration

- CVE-2016-1997

HP Asset Manager

- CVE-2016-2000

HP Service Manager

- CVE-2016-1998

HP Operations Manager

- CVE-2016-1985

HP Release Control

- CVE-2016-1999

HP Continuous Delivery Automation

- CVE-2016-1986

HP P9000, XP7 Command View Advanced Edition (CVAE) Suite

- CVE-2016-2003

HP Network Automation

- CVE-2016-4385

Adobe Experience Manager

- CVE-2016-0958

Unify OpenScape (various)

- CVE-2015-8237
- RMI (30xx/tcp)
- CVE-2015-8238
- js-soc protocol (4711/tcp)

Apache OFBiz

- CVE-2016-2170

Apache Tomcat

- 需要本地访问
- CVE-2016-0714
- Article

Apache TomEE

- CVE-2015-8581
- CVE-2016-0779

IBM Congnos BI

- CVE-2012-4858

Novell NetIQ Sentinel

- ?

ForgeRock OpenAM

- 9-9.5.5, 10.0.0-10.0.2, 10.1.0-Xpress, 11.0.0-11.0.3 and 12.0.0
- 201505-01

F5 (various)

- sol30518307

Hitachi (various)

- HS16-010
- 0328_acc

NetApp (various)

- CVE-2015-8545

Zimbra Collaboration

- < 8.7.0
- CVE-2016-3415

Adobe ColdFusion

- <= 2016 Update 5
- <= 11 update 13
- CVE-2017-11283
- CVE-2017-11284

Code42 CrashPlan

- TCP port 4282
- RMI (?)
- 5.4.x
- CVE-2017-9830
- Details

Apache Batchee

Apache JCS

Apache OpenJPA

Apache OpenWebBeans

防御工具

- 反序列化安全优化
- NotSoSerial
- 反序列化静默器
- ObjectInputStream检测器
- 名称空间布局随机化
- 绕过防护tips
- Tool: Serial Whitelist Application Trainer
- JEP 290: 过滤传入的序列化数据 in JDK 6u141, 7u131, 8u121

For Android

- Android中的0day反序列化漏洞
- Android序列化漏洞重新审视

XMLEncoder (XML)

攻击原理

- http://blog.diniscruz.com/2013/08/using-xmldecoder-to-execute-server-side.html
- Java Unmarshaller Security

Exploits:

Oracle Weblogic

- <= 10.3.6.0.0
- <= 12.1.3.0.0
- <= 12.2.1.2.0
- <= 12.2.1.1.0
- http://weblogic_server/wls-wsat/CoordinatorPortType
- CVE-2017-3506
- CVE-2017-10271
- Details

Exploit

XStream (XML/JSON/various)

攻击原理

- http://www.pwntester.com/blog/2013/12/23/rce-via-xstream-object-deserialization38/
- http://blog.diniscruz.com/2013/12/xstream-remote-code-execution-exploit.html
- https://www.contrastsecurity.com/security-influencers/serialization-must-die-act-2-xstream
- Java Unmarshaller Security

Payload 生成器

- https://github.com/mbechler/marshalsec

Exploits:

Apache Struts (S2-052)

- <= 2.3.34
- <= 2.5.13
- REST plugin
- CVE-2017-9805

Exploit

被黑掉的应用 (without public sploits/need more info):

Atlassian Bamboo

- CVE-2016-5229

Jenkins

- CVE-2017-2608

Kryo (binary)

如何黑掉它

- https://www.contrastsecurity.com/security-influencers/serialization-must-die-act-1-kryo
- Java Unmarshaller Security

Payload 生成器:

- https://github.com/mbechler/marshalsec

Hessian/Burlap (binary/XML)

攻击原理

- Java Unmarshaller Security

Payload 生成器

- https://github.com/mbechler/marshalsec

Castor (XML)

攻击原理

- Java Unmarshaller Security

Payload 生成器

- https://github.com/mbechler/marshalsec

被黑掉的应用(without public sploits/need more info):

OpenNMS

- NMS-9100

json-io (JSON)

攻击原理

- Java Unmarshaller Security

Payload 生成器

- https://github.com/mbechler/marshalsec

Jackson (JSON)

vulnerable in some configuration

攻击原理

- Java Unmarshaller Security

Payload 生成器

- https://adamcaudill.com/2017/10/04/exploiting-jackson-rce-cve-2017-7525/
- https://github.com/mbechler/marshalsec

被黑掉的应用(without public sploits/need more info):

Apache Camel

- CVE-2016-8749

Red5 IO AMF (AMF)

攻击原理

- Java Unmarshaller Security

Payload 生成器

- https://github.com/mbechler/marshalsec

被黑掉的应用(without public sploits/need more info):

Apache OpenMeetings

- CVE-2017-5878

Apache Flex BlazeDS (AMF)

攻击原理

- AMF – Another Malicious Format
- Java Unmarshaller Security

Payload 生成器

- https://github.com/mbechler/marshalsec

被黑掉的应用(without public sploits/need more info):

Adobe ColdFusion

- CVE-2017-3066
- <= 2016 Update 3
- <= 11 update 11
- <= 10 Update 22

Apache BlazeDS

- CVE-2017-5641

VMWare VCenter

- CVE-2017-5641

Flamingo AMF (AMF)

攻击原理

- AMF – Another Malicious Format

GraniteDS (AMF)

攻击原理

- AMF – Another Malicious Format

WebORB for Java (AMF)

攻击原理

- AMF – Another Malicious Format

SnakeYAML (YAML)

攻击原理

- Java Unmarshaller Security

Payload 生成器

- https://github.com/mbechler/marshalsec

被黑掉的应用(without public sploits/need more info):

Resteasy

- CVE-2016-9606

Apache Camel

- CVE-2017-3159

Apache Brooklyn

- CVE-2016-8744

jYAML (YAML)

攻击原理

- Java Unmarshaller Security

Payload 生成器

- https://github.com/mbechler/marshalsec

YamlBeans (YAML)

攻击原理

- Java Unmarshaller Security

Payload 生成器

- https://github.com/mbechler/marshalsec

"Safe" deserialization

一些序列化库是安全的（或几乎安全https://github.com/mbechler/marshalsec

但这不是官方建议，而是由一个安全研究员提出的建议列表：

- JAXB
- XmlBeans
- Jibx
- ProtobufGSON
- GWT-RPC

上一篇：Java反序列化漏洞从入门到深入 下一篇：Java反序列化漏洞之殇
1. 1 条回复

 younge 2018-03-03 13:38:30

反序列化漏洞引发的信息泄露

这里翻译有问题吧，意思都改了
原文意思应该是
用反序列化黑掉Java消息服务

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板