信息泄露之配置不当——安全小课堂第六期

京东安全应急响应应中心 2016-04-15

安全小课堂第六期

信息泄露涉及范围广泛，破坏之大，给业内各企业带来不少担忧与苦恼。本期我们来重点聊一聊由于配置不当导致的信息泄露。

今天邀请到百度高级研究员胡飞和唯品会高级研究员feng为大家分享本期主题，掌声响起来~😳😳

1

豌豆妹

配置不当的分类有哪些呢？

哆啦A梦 

分类是见仁见智的。
一般根据发生场景进行大致分类，比如（1）webserver本身：之前发生的nginx等解析漏洞，webserver的目录遍历等。（2）网络协议相关：snmp弱community、dns域传送、ssh等。（3）应用相关：压缩文件，备份文件，其他如日志history、phpinfo等，zabbix，jenkins、phpmyadmin、hadoop等。（4）系统相关：之前暴露的openssl心脏滴血，破壳等。

豌豆妹

哪类引发的危害比较大呢？

哪类引发的危害比较大呢？

小丸子

这些因为配置不当引发的问题很容易导致大事件。但其后果的严重与否，可能还是要根据具体的业务场景来看。一般来说geshell算是很严重了。

葫芦娃

个人认为，每种分类如果被利用都可以造成很大危害，比如svn，git信息泄露可导致代码泄露，从而可以进行白盒代码审计，一旦代码存在漏洞是很容易被白盒挖掘出来。比如经典的nginx+php cgi，当误配置cgi.fix_pathinfo=1话，会存在文件解析问题
http://www.oxen.com/evil.jpg/test.php，通过正则匹配，script_name会被设置为evil.jpg/test.php，然后传递给 php cgi，php会认为script_name为evil.jpg，而test.php为path_info，然后php把evil.jpg当做一个php文件来解析执行。

2

豌豆妹

配置不当导致的漏洞如何定级？

小新

定级需要根据业务和场景进行定义，主要还是看漏洞对业务的影响。

小丸子

我之前刚好有整理过相关信息，既然聊到这儿，我就把一些资料发出来吧。
解析漏洞：nginx、apache、IIS
危害：潜在getshell
工具：http://drops.wooyun.org/papers/539

3

豌豆妹

配置不当的防范，大家是否有好的措施来分享？

哆啦A梦

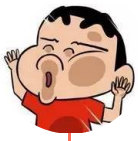
针对配置不当的防范，当前的做法是：1、业务上线前进行安全基线检查。2、对线上业务进行定时检查。3、对攻击行为进行监控。一般这样做之后会杜绝大部分的配置不当问题， 其他信息泄露问题主要是采用自检或者src白帽子提交的漏洞来发现，发现之后走修复流程，不会分层做。

小新

基本上就是：培训+监控，辅助扫描。比如开发阶段，会制定公司的安全配置基线要求及安全配置关注点，通过安全教育培训来提高op等安全意识，甚至可以通过安全知识小卡片进行相应宣传。此外，统一安全配置基线，即最低安全红线，根据安全配置基线产生公司默认配置模板，所有预上线阶段全部默认使用配置模板，当模板满足不了需求时，可以根据配置模板进行相应更改，但是上线之前需要通过安全基线工具check。

豌豆妹

安全工具是集成在上线的某个位置，还是独立外部检查？

小新 

刚才的分类其实大部分都在例行check中，当然目前还在补充中。

葫芦娃 

我们是通过主机agent进行。通过agent，一旦监控到关心的配置文件，比如webserver配置文件有更改，立刻通过agent进行相应check，看是否违背了安全配置基线，若违背了，则给出默认整改时间；如果负责人在规定的整改时间以内未修改，工具自动按照安全要求将不规范点修改回来。

4

豌豆妹

举个例子，研发人员在上迭代版本的时候可能考虑回滚方便，然后在目录中打了个back，导致外部可以打包拿走。这种情况大家有好的方法吗？

小新 

我理解这种，可以在两个点check，一是代码上线流程中，一种就是线上针对webserver目录的监控进行。

豌豆妹

业内是否有检测配置不当方面比较棒的工具和模块方法呢？

小丸子 

最近看到一个开源工具，还是不错的。
其他各种已知漏洞：
比如说jboss的各种geshell漏洞、redis任意文件读取...
工具：https://github.com/ywolf/F-MiddlewareScan

葫芦娃 

目前模块还是比较少，大家可以自己开发插件加入。

豌豆妹

如何对攻击行为进行监控？

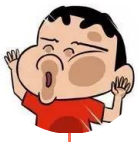
小丸子 

主要是通过海量日志的分析，从中抓取特征进行预警。日志分析依托于soc系统，soc

还是我们对抗黄牛党、羊毛党的重要武器。此外，在生产服务器上也有webshell实时监测等。

豌豆妹

对于类似“脱裤”行为的泄露有好的方案吗?

小新 

目前针对“脱裤”，我们这边在两个方面做了监控，一个waf层面，一个是db层面，就是我们这边所有数据库都是通过proxy方式进行，会实时收集到sql日志，然后根据日志进行判断，及时阻断。

豌豆妹

代理那块怎么实现呢？

葫芦娃 

其实可以简单理解类似一个应用和db的代理，主要做日志记录，授权认证等。看下面这个图，就可以一目了然~

豌豆妹

一个有趣的问题：我们怎么才能从外部谣传的泄露库来判断是否为本公司的库，而不是撞出来的，并基本能够定位时间？

哆啦A梦 

这个需要根据日志分析，然后逐步定位。

葫芦娃 

立flag，设置几个虚假的账号，账号某些信息根据当天时间对应。

JSRC http://security.jd.com/

长按识别左侧二维码，关注我们