

腾讯云Web漏洞扫描报告

安全等级：**高危**

2018.12.14



腾讯云

【注意】

本报告包含机密信息，不得通过电子邮件、传真、或其它电子设备进行传播，不得对该文档做任何副本或者备份。除非经过授权，否则不得向任何人共享该文档内的任何信息。

文档目录

1 基本信息

2 扫描结果摘要

2.1 漏洞类型分布

2.2 存在漏洞的URL

3 漏洞详细信息

1 基本信息

扫描结果



网站地址	http://jianke.ocean-ad.com.cn/
风险等级	高危
漏洞数量	1个高危漏洞, 2个提示
扫描模式	深度扫描
扫描速率	10个HTTP请求每秒
扫描完成时间	2018-12-14 10:32:10

2 扫描结果摘要

安全等级	漏洞总数	高危漏洞	中危漏洞	低危漏洞	风险提示
高危	3	1	0	0	2

2.1 漏洞类型分布

等级	漏洞类型	漏洞数量
高危	Serv-U FTP服务器权限绕过漏洞 (CVE-2011-4800)	1
提示	FTP Service Enable	1
提示	Windows Terminal Services Port 3389 Enabled	1

2.2 存在漏洞的URL

等级	URL
高危	Serv-U Jail Break jianke.ocean-ad.com.cn:21 (FTP Banner:Serv-U FTP Server v...
提示	Windows Terminal Services Port 3389 Enabled (host:jianke.ocean-ad.com.cn)
提示	jianke.ocean-ad.com.cn:21 (FTP Banner:Serv-U FTP Server v6.4 for WinSock re...

3 漏洞详细信息

漏洞 1

漏洞类型:	Serv-U FTP服务器权限绕过漏洞 (CVE-2011-4800)
漏洞等级:	高危
出现漏洞的URL:	Serv-U Jail Break jianke.ocean-ad.com.cn:21 (FTP Banner:Serv-U FTP Server v6.4 for WinSock ready...)
漏洞描述:	影响版本:Serv-U FTP Server 版本号 低于 11.1.0.5。 RhinoSoft Serv-U FTP Server实现上存在目录遍历漏洞，通过输入特定的路径串可以实现目录遍历，攻击者可以下载、上传、删除FTP根目录外的文件。
解决方案:	Linux/Unix解决方案:Linux不存在该软件。 Windows解决方案:升级Serv-U FTP Server到最新版本。
漏洞危害:	RhinoSoft Serv-U FTP Server实现上存在目录遍历漏洞，通过输入特定的路径串可以实现目录遍历，攻击者可以下载、上传、删除FTP根目录外的文件。
漏洞参考:	OWASP:不适用 WASC:不适用 CVE: CVE-2011-4800 CWE:不适用 OSVDB-ID: 77422

漏洞 2

漏洞类型:	FTP Service Enable
漏洞等级:	提示
出现漏洞的URL:	jianke.ocean-ad.com.cn:21 (FTP Banner:Serv-U FTP Server v6.4 for WinSock ready...)
漏洞描述:	在该服务器上发现敏感服务端口对外开放存在风险，容易引起安全问题
解决方案:	关闭非必需的服务端口，如是必需开放端口，建议修改其默认端口更改为高位端口
漏洞危害:	在该服务器上发现敏感服务端口对外开放存在风险，容易引起安全问题
漏洞参考:	暂无相关信息

漏洞 3

漏洞类型:	Windows Terminal Services Port 3389 Enabled
漏洞等级:	提示
出现漏洞的URL:	Windows Terminal Services Port 3389 Enabled (host:jianke.ocean-ad.com.cn)
漏洞描述:	在该服务器上发现敏感服务端口对外开放存在风险, 容易引起安全问题
解决方案:	关闭非必需的服务端口, 如是必需开放端口, 建议修改其默认端口更改为高位端口
漏洞危害:	在该服务器上发现敏感服务端口对外开放存在风险, 容易引起安全问题
漏洞参考:	暂无相关信息