关于宝塔 Windows 面板默认存在 IIS 解析漏洞的情况告警

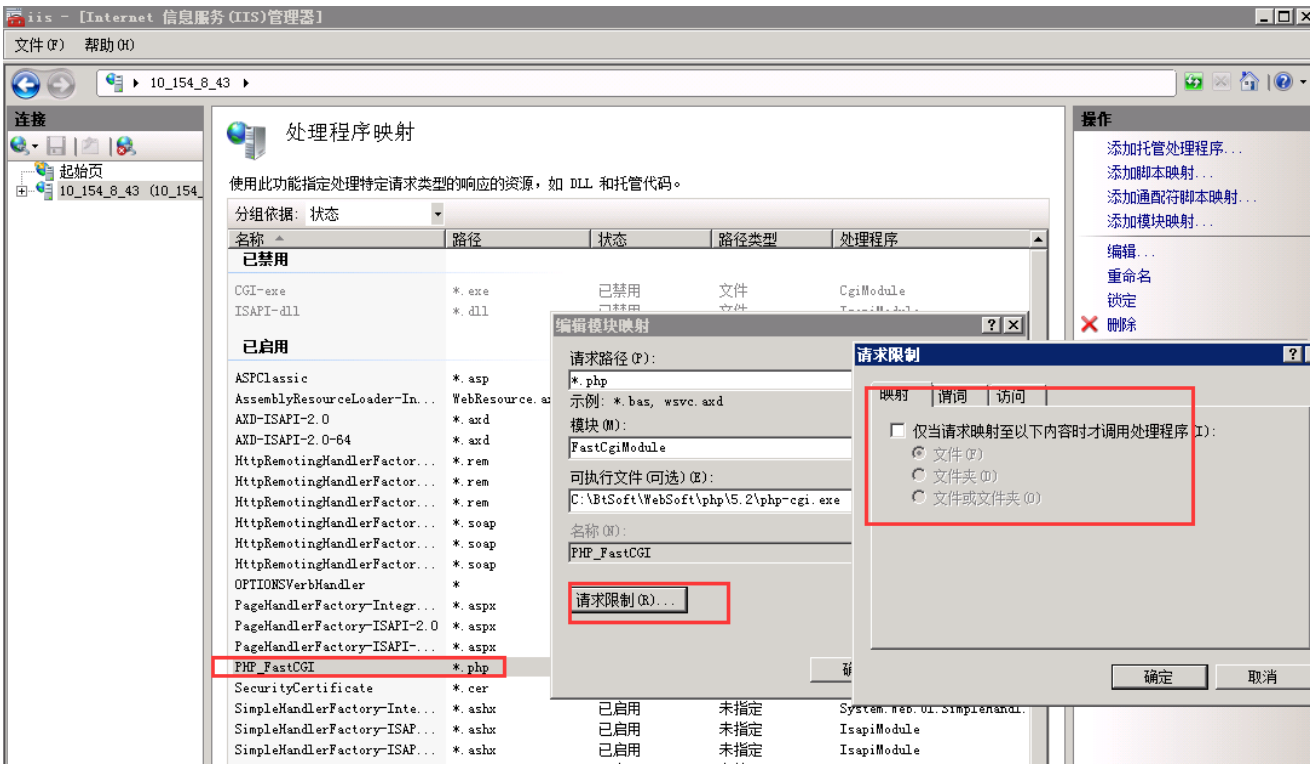
1. 背景

宝塔 Windows 面板是一款专业的服务器管理产品，用户可以方便的利用宝塔 Windows 面板的管理控制台创建、删除、管理网站，同时可以确保服务器安全性。宝塔 Windows 面板同时在腾讯云提供了宝塔 Windows 面板镜像，腾讯云用户可以快捷的创建一个安装了宝塔 Windows 面板的主机来进行建站管理。

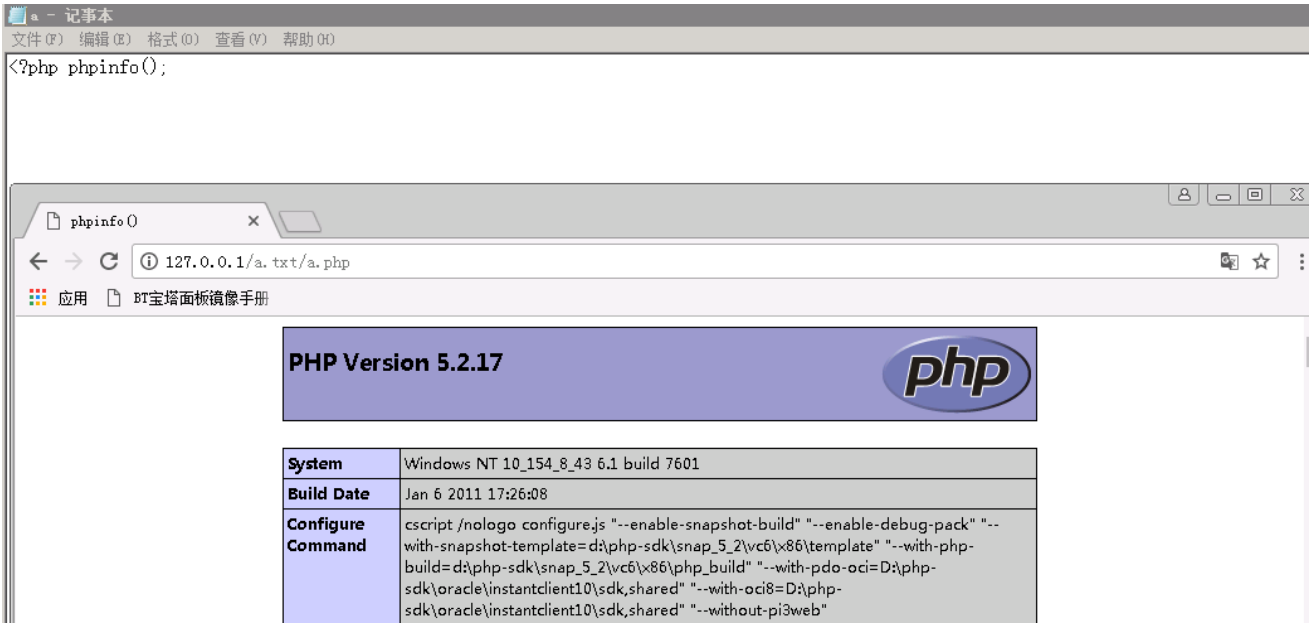
腾讯安全云鼎实验室在日常安全运营中发现，宝塔 Windows 面板默认安装的 IIS+PHP 环境存在 IIS 解析漏洞，攻击者可以在任意文件上传点上传一个包含着恶意 PHP 代码的文件（图片、TXT、压缩包等）后，通过利用 IIS 解析漏洞即可执行 PHP 代码，可能会导致用户代码、数据库泄露。

2. 漏洞详情

宝塔 Windows 面板安装的 IIS 服务是利用 IIS 处理程序映射处理 *.php 的文件，具体配置详情如下图：



如图所示，对于 *.php 的请求，其请求限制未设置映射。即当请求到任意 URI（包括不存在的资源）时，也会映射至 FastCGI 进行处理。于此同时，宝塔 Windows 面板默认安装的 PHP 的配置中，其 cgi.fix_pathinfo 配置项为 1（默认值）。当 **cgi.fix_pathinfo 为 1 且 IIS 的请求限制映射未配置成为文件**时，就会产生 IIS 解析漏洞：



利用此漏洞需要结合用户的业务，如用户利用宝塔 Windows 面板安装了一个 PHP 的论坛，利用论坛上传图片处上传一个恶意且合法的图片，再利用解析漏洞去请求这个文件，即可执行 PHP 代码。

3. 修复建议

针对此漏洞，不推荐修改 php.ini 进行修复，推荐的是设置 IIS 的处理请求映射中，*.php 的映射的请求限制为文件即可修复此漏洞：