绿盟科技"远程安全评估系统"安全评估报告-主机报表

报表生成时间 2023-02-24 10:09:12

目录

1 主机概况 1

2 漏洞信息 1

3 其他信息 5

4 对比分析 6

5 参考标准 7

1 主机概况

主机风险	非常危险(9.9分)
IP地址	166.111.156.3
操作系统	Linux 3.10 - 4.11
系统版本	V6.0R04F02SP02
插件版本	V6.0R02F01.2909
扫描起始时间	2023-02-20 16:58:13
扫描结束时间	2023-02-20 17:31:02
漏洞扫描检查模板	自动匹配扫描
漏洞风险评估分	9.9
主机风险评估分	9.9

2 漏洞信息

2.1 漏洞概况

远程扫描			
端口	**协议**	**服务**	**漏洞**
80	TCP	http	PHP 拒绝服务安全漏洞(CVE-2018-19396) PHP 安全漏洞(CVE-2019-9641) PHP远程命令执行漏洞(CVE-2022-31625) PHP 安全漏洞(CVE-2015-9253)

2.2 漏洞详情

漏洞名称	PHP 拒绝服务安全漏洞(CVE-2018-19396)
详细描述	该漏洞为远程版本检测，存在误报风险。 PHP是一种开源的通用计算机脚本语言。该语言主要用于Web开发，支持多种数据库及操作系统。 PHP 5.x版本至7.1.24版本，在ext/standard/var_unserializer.c文件存在安全漏洞。攻击者可利用该漏洞造成拒绝服务（应用程序崩溃）。
解决办法	厂商补丁: PHP --- 目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载： https://bugs.php.net/bug.php?id=77177
威胁分值	7.5
危险插件	否
发现日期	2018-11-22
CVE编号	CVE-2018-19396
NSFOCUS	41988
CNNVD编号	CNNVD-201811-620
CNCVE编号	CNCVE-201819396
CVSS评分	5.0

漏洞名称	PHP 安全漏洞(CVE-2019-9641)
详细描述	PHP（PHP：Hypertext Preprocessor，PHP：超文本预处理器）是PHPGroup和开放源代码社区的共同维护的一种开源的通用计算机脚本语言。该语言主要用于Web开发，支持多种数据库及操作系统。EXIF component是其中的一个可交换图像文件格式处理组件。 PHP 7.1.27之前版本、7.2.16之前的7.2.x版本和7.3.3之前的7.3.x版本中的EXIF组件的 ‘exif_process_IFD_in_TIFF’ 函数存在安全漏洞。
解决办法	厂商补丁: PHP --- 目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载： https://bugs.php.net/bug.php?id=77509
威胁分值	9.8
危险插件	否
发现日期	2019-03-08
CVE编号	CVE-2019-9641
CNNVD编号	CNNVD-201903-313
CNCVE编号	CNCVE-20199641
CVSS评分	7.5
CNVD编号	CNVD-2019-24790

漏洞名称	PHP远程命令执行漏洞(CVE-2022-31625)
详细描述	PHP是一种在服务器端执行的脚本语言。 在 PHP_FUNCTION 中分配在堆上的的 char* 数组没有被清除，如果发生转换错误，将会调用_php_pgsql_free_params()函数，由于数组没有初始化，导致可以释放之前请求的值，导致远程代码执行。 受影响版本： 5.3.0 <= PHP 5.x <= 5.6.40 7.0.1 <= PHP 7.x < 7.4.30 8.0.0 <= PHP 8.0.x < 8.0.20 8.1.0 <= PHP 8.1.x < 8.1.7
解决办法	厂商补丁: 目前厂商已发布升级补丁以修复漏洞，补丁获取链接： https://www.php.net/
威胁分值	8.1
危险插件	否
发现日期	2022-06-08
CVE编号	CVE-2022-31625
CNNVD编号	CNNVD-202206-932
CNCVE编号	CNCVE2022-31625
CVSS评分	6.8

漏洞名称	PHP 安全漏洞(CVE-2015-9253)
详细描述	PHP（PHP：Hypertext Preprocessor，PHP：超文本预处理器）是PHP Group和开放源代码社区共同维护的一种开源的通用计算机脚本语言。该语言主要用于Web开发，支持多种数据库及操作系统。 PHP 7.2.2及之前的版本中存在安全漏洞。攻击者可利用该漏洞耗尽CPU资源并消耗磁盘空间。

解决办法	厂商补丁: PHP ------- 目前厂商已发布升级补丁以修复漏洞，补丁获取链接： http://php.net/
威胁分值	6.5
危险插件	否
发现日期	2018-02-19
CVE编号	CVE-2015-9253
CNNVD编号	CNNVD-201802-805
CNCVE编号	CNVE-20159253
CVSS评分	6.8

3 其它信息

3.1 远程端口信息

端口	协议	服务	状态
80	tcp	http	open
21	tcp	ftp	open
22	tcp	ssh	open
888,12002	tcp	www	open

3.2 安装软件信息

软件名称	版本号
FTP	220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 1 of 50 allowed.220-Local time is now 17:08. Server port: 21.220-This is a private system - No anonymous login220-IPv6 connections are also welcome on this server.220 You will be disconnected after 15 minutes of inactivity.
WWW	nginx
Pure-FTPd	
nginx	
OpenSSH	7.4
nginx;PHP	5.6.40
Ajenti http control panel	
220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 1 of 50 allowed.220-Local time is now 17:08. Server port: 21.220-This is a private system - No anonymous login220-IPv6 connections are also welcome on this server.220 You will be disconnected after 15 minutes of inactivity.	
SSH	SSH-2.0-OpenSSH_7.4

PHP	5.6.40
SSH Server	SSH-2.0-OpenSSH_7.4

3.3 操作系统类型

操作系统名字	版本号
Linux	3.10 - 4.11

3.4 端口Banner

端口	Banner
22	OpenSSH/7.4
888	nginx
12002	nginx
80	nginx;PHP/5.6.40
21	220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 1 of 50 allowed.220-Local time is now 17:08. Server port: 21.220-This is a private system - No anonymous login220-IPv6 connections are also welcome on this server.220 You will be disconnected after 15 minutes of inactivity.

4 对比分析

4.1 任务对比分析

5 参考标准

5.1 单一漏洞风险等级评定标准

危险程度	危险值区域	危险程度说明
高	7 <= 漏洞风险值 <=10	攻击者可以远程执行任意命令或者代码，或对系统进行远程拒绝服务攻击。
中	4 <= 漏洞风险值 < 7	攻击者可以远程创建、修改、删除文件或数据，或对普通服务进行拒绝服务攻击。
低	0 <= 漏洞风险值 < 4	攻击者可以获取某些系统、服务的信息，或读取系统文件和数据。

说明：

漏洞的风险值兼容CVSS评分标准。

5.2 主机风险等级评定标准

主机风险等级	主机风险值区域
非常危险	7.0 <= 主机风险值 <= 10.0
比较危险	5.0 <= 主机风险值 < 7.0
比较安全	2.0 <= 主机风险值 < 5.0
非常安全	0.0 <= 主机风险值 < 2.0

说明：

1. 按照远程安全评估系统的主机风险评估模型计算主机风险值。根据得到的主机风险值参考“主机风险等级评定标准”标识主机风险等级。
2. 将主机风险等级按照风险值的高低进行排序，得到非常危险、比较危险、比较安全、非常安全四种主机风险等级。
3. 用户可以根据自己的需要修订主机风险等级中的主机风险值范围。