T1060部分威胁日志含义

Syslog日志 刘宏宇 2019-11-25 发表

问题描述

T1060 如下威胁日志含义：

WEB_SERVER_PyCurl_Suspicious_User_Agent_Inbound
Web_Applications_SQL_Injection_Attack_Get(Boolean)
NSFOCUS_RSAS_Get_Bind_Version_Attempt(UDP)
Apache_Struts2_includeParams_Attribute_Remote_Commond_Execution_Vulnerability(POST)
Generic_XSS_Attack(Script_RawHeader)
SCAN_Non-Allowed_Host_Tried_to_Connect_to_MySQL_Server
Web_Applications_SQL_Injection_Attack_Get(Boolean)
DNS_Query_to_a_.tk_domain_-_Likely_Hostile
(CVE-2014-4049)PHP_DNS_TXT_Record_Handling_Heap_Buffer_Overflow_Vulnerability

解决方法

WEB_SERVER_PyCurl_Suspicious_User_Agent_Inbound

9602 WEB_SERVER_PyCurl_Suspicious_User_Agent_Inbound 针对WEB服务器User_Agent为PyCurl的可疑访问 PyCurl是一个C语言写的libcurl库的封装，是一个自由的容易使用的客户端URL传输库。该规则用于发现WEB服务器User_Agent为PyCurl的可疑访问请求。 目前官方还没有提供相应补丁，请密切关注官方更新。 RS01 NA NA NA NA true Permit+Logging

Web_Applications_SQL_Injection_Attack_Get(Boolean)

24320 Web_Applications_SQL_Injection_Attack_Get(Boolean) Web_Applications_SQL_Injection_Attack_Get(Boolean) SQL Injection is a technique used to take advantage of non-validated input vulnerabilities to pass SQL commands through a Web application for execution by a backend database. This signature detects SQL injection attacks involving the Boolean SQL statement. 目前官方还没有提供相应补丁，请密切关注官方更新。 RS01 NA NA NA NA true Permit+Logging

NSFOCUS_RSAS_Get_Bind_Version_Attempt(UDP)

17476 NSFOCUS_RSAS_Get_Bind_Version_Attempt(TCP) NSFOCUS_RSAS_Get_Bind_Version_Attempt(TCP) NSFOCUS_RSAS_Get_Bind_Version_Attempt(TCP) 目前官方还没有提供相应补丁，请密切关注官方更新。 RS01 NA NA NA NA true BlockSrc+Logging

Apache_Struts2_includeParams_Attribute_Remote_Commond_Execution_Vulnerability(POST)

243

Apache_Struts2_includeParams_Attribute_Remote_Commond_Execution_Vulnerability(POST)

Apache_Struts2_includeParams属性远程命令执行漏洞(POST) Microsoft Internet Information Services是由微软公司提供的基于运行Microsoft Windows的互联网基本服务。Microsoft Internet Information Services (IIS) 7.5版本中存在缓冲区溢出漏洞。当FastCGI功能的IIS服务器启用时，远程攻击者可以借助特制请求头执行任意代码。 目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商主页下载：http://www.microsoft.com/technet/security/Bulletin/MS10-065.mspx RS01 CVE-2013-1966,CVE-2013-4316,CVE-2013-2115 60166,62587,60167 NA CNNVD-201305-493,CNNVD-201309-445,CNNVD-201305-577 true Reset+Logging

Generic_XSS_Attack(Script_RawHeader)

31627 Generic_XSS_Attack(Script_RawHeader) Generic_XSS_Attack(Script_RawHeader) Generic_XSS_Attack(Script_RawHeader) 目前官方还没有提供相应补丁，请密切关注官方更新。 RS01 NA NA NA NA true Reset+Logging

SCAN_Non-Allowed_Host_Tried_to_Connect_to_MySQL_Server

11395 SCAN_Non-Allowed_Host_Tried_to_Connect_to_MySQL_Server 针对MYSQL服务器的尝试连接扫描 针对MYSQL服务器的尝试连接扫描 目前官方还没有提供相应补丁，请密切关注官方更新。 RS01 NA NA NA NA true Permit+Logging

Web_Applications_SQL_Injection_Attack_Get(Boolean)

24320 Web_Applications_SQL_Injection_Attack_Get(Boolean) Web_Applications_SQL_Injection_Attack_Get(Boolean) SQL Injection is a technique used to take advantage of non-validated input vulnerabilities to pass SQL commands through a Web application for execution by a backend database. This signature detects SQL injection attacks involving the Boolean SQL statement. 目前官方还没有提供相应补丁，请密切关注官方更新。 RS01 NA NA NA NA true Permit+Logging

DNS_Query_to_a_.tk_domain_-_Likely_Hostile

19278 DNS_Query_to_a_.tk_domain_-_Likely_Hostile 针对.tk域中主机的可疑DNS请求 针对.tk域中主机的可疑DNS请求 目前官方还没有提供相应补丁，请密切关注官方更新。 RS01 NA NA NA NA false Permit+Logging

(CVE-2014-4049)PHP_DNS_TXT_Record_Handling_Heap_Buffer_Overflow_Vulnerability

PHP_DNS_TXT_Record_Handling_Heap_Buffer_Overflow_Vulnerability (CVE-2014-4049)PHP基于堆的缓冲区溢出漏洞 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。该语言支持多重语法、支持多数据库及操作系统和支持C、C++进行程序扩展等。PHP 5.6.0beta4及之前版本的ext/standard/dns.c文件中的'php_parserr'函数存在基于堆的缓冲区溢出漏洞。远程攻击者可借助特制的DNS TXT记录利用该漏洞造成拒绝服务（崩溃）。 目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商主页下载:http://www.php.net/ RS02 CVE-2014-4049 NA NA CNNVD-201406-432 true Drop+Logging