Workspace是否涉及Samba相关漏洞CVE-2010-2063&CVE-2010-3069&CVE-2012-1182&CVE-2010-1635&CVE-2010-1642

戴丽丽 2021-08-23 发表

漏洞相关信息

漏洞编号： CVE-2010-2063/CVE-2010-3069/CVE-2012-1182/CVE-2010-1635/CVE-2010-1642
漏洞名称： Samba相关漏洞
产品型号及版本： E1009

漏洞描述

1、Samba SMB1报文链接远程内存破坏漏洞(CVE-2010-2063)
Samba 3.0.x 3.3.13之前版本中smbd中process.c中的chain_reply函数中的SMB1数据包链接实现存在缓冲区溢出，远程攻击者可借助数据包中的特制字段造成拒绝服务（内存损坏和守护程序崩溃）或可能执行任意代码。
2、Samba sid_parse和dom_sid_parse函数栈缓冲区错误漏洞(CVE-2010-3069)
Samba 3.5.5之前版本中的（1）sid_parse和（2）dom_sid_parse函数中存在基于堆栈的缓冲区溢出，远程攻击者可借助文件共享上特制的Windows安全ID（sid）造成拒绝服务（崩溃）并可能执行任意代码。
3、Samba任意代码执行漏洞(CVE-2012-1182)
Samba 3.4.16之前的3.x版本、3.5.14之前的3.5.x版本和3.6.4之前的3.6.x版本中的RPC代码生成器中存在漏洞，该漏洞源于未实现以验证数组内存分配的方式对数组长度进行验证。
4、Samba Smbd守护程序chain_reply函数拒绝服务漏洞(CVE-2010-1635)
Samba 3.4.8之前版本的smbd中process.c和3.5.2之前版本的3.5.x中的chain_reply函数允许远程攻击者通过具有特定0x0003字段值的协商协议请求，然后是会话设置和具有特定0x8003字段值的x请求，造成拒绝服务（空指针解引用和进程崩溃）。
5、Samba Smbd守护程序 reply_sesssetup_and_X_spnego函数拒绝服务漏洞(CVE-2010-1642)
Samba 3.4.8之前的版本和3.5.2之前的版本中的smbd中的sessetup.c中的reply_sessetup_和_X_spnego函数允许远程攻击者通过会话设置和X请求中的\xff\xff安全blob长度触发越界读取，并导致拒绝服务（进程崩溃）。

漏洞解决方案

E1009环境Samba版本为4.10.17，上述漏洞涉及版本为3.x.x，ws不涉及Samba相关漏洞。