Samba 远程代码执行漏洞

(CVE-2017-7494)

安全预警通告

360安全监测与响应中心

2017 年 05 月 25 日

目录

第 1 章 安全通告 3

第 2 章 事件信息 4

2.1 事件描述 4
2.2 风险等级 4

第 3 章 处置建议 5

3.1 确认影响范围 5
3.2 应急处置手段 5
3.3 快速应急处置建议 6
3.4 官方建议 6

第 4 章 技术分析 7

4.1 具体攻击过程 8
4.2 攻击结果 8

第 5 章 参考文档 11

第1章 安全通告

尊敬的客户：

2017 年 5 月 24 日 Samba 服务器软件发布了最新的 4.6.4 版本，修复了一个严重的远程代码执行漏洞，漏洞编号为 CVE-2017-7494。360 网络安全中心和 360 信息安全部的 Gear Team 第一时间对该漏洞进行了分析，在有低权限账号登录到系统并且有可写共享的条件下，可以造成服务器以 root 用户权限执行攻击指定的恶意代码。此漏洞在通常的 Samba 服务器场景下，导致权限提升攻击，在某些默认权限配置松懈的 NAS 系统中可能导致远程命令执行。

此漏洞影响 Samba 3.5.0 及以后的版本，在 4.6.4、4.5.10、4.4.14 及以后的版本中被修复。

Samba 是在 Linux 和 Unix 系统上实现 SMB 协议的一个免费软件，由服务器及客户端程序构成。SMB（Server Messages Block，信息服务块）是一种在局域网上共享文件和打印机的一种通信协议，它为局域网内的不同计算机之间提供文件及打印机等资源的共享服务。SMB 协议是客户机/服务器型协议，客户机通过该协议可以访问服务器上的共享文件系统、打印机及其他资源。通过设置“NetBIOS over TCP/IP”使得 Samba 不但能与局域网络主机分享资源，还能与全世界的电脑分享资源。

360 安全监测与响应中心也将持续关注该漏洞进展，并在第一时间为您更新该漏洞信息。

第2章 事件信息

2.1 事件描述

2017 年 5 月 24 日 Samba 服务器发布了 4.6.4 版本，修复了一个严重安全漏洞，分析确认此漏洞在一定条件下可以被用来执行远程恶意代码，导致权限提升或远程控制服务器，需要尽快采取应对措施。

2.2 风险等级

360 安全监测与响应中心风险评级为：严重

第3章 处置建议

3.1 确认影响范围

受影响的版本：

Samba 版本 >= 3.5.0

不受影响的版本

Samba 版本 >= 4.6.4

Samba 版本 >= 4.5.10

Samba 版本 >= 4.4.14

3.2 应急处置手段

360 网络安全响应中心和 360 信息安全部建议使用受影响版本的用户立即通过以下方式来进行安全更新操作：

1. 使用源码安装的 Samba 用户，请尽快下载最新的 Samba 版本手动更新；

2. 使用二进制分发包（RPM 等方式）的用户立即进行 yum，apt-get update 等安全更新操作。

3. 360 新一代智慧防火墙（NSG3000/5000/7000/9000 系列）和下一代极速防火墙（NSG3500/5500/7500/9500 系列）产品系列，已通过更新 IPS 特征库完成了对上述攻击工具相关漏洞的防护。**建议用户尽快将 IPS 特征库升级至“20170525”版本并启用规则 ID：50793 进行防护**

4. 360 天眼未知威胁感知系统的流量探针已第一时间加入了对该漏洞（CVE-2017-7494）的支持。建议用户尽快将流量探针的规则引擎升级至最新版本：3.0.0525.10457，对应规则 ID: 0x4a61。对于发现的攻击，可以在 360 天眼分析平台上实时看到相应告警。

请在系统配置->设备升级->规则升级，点击“网络升级”或者“本地升级”。

3.3 快速应急处置建议

用户可以通过在 smb.conf 的[global]节点下增加 nt pipe support = no 选项，然后重新启动 samba 服务，以此达到缓解针对该漏洞攻击的效果。

3.4 官方建议

Samba 官方已经提供了新版本来修复上述漏洞，请受影响的用户尽快升级到新版本，下载链接如下：

https://download.samba.org/pub/samba/stable/samba-4.6.4.tar.gz

https://download.samba.org/pub/samba/stable/samba-4.5.10.tar.gz

https://download.samba.org/pub/samba/stable/samba-4.4.14.tar.gz

第4章 技术分析

如官方所描述，该漏洞只需要通过一个可写入的 Samba 用户权限就可以提权到 samba 所在服务器的 root 权限（samba 默认是 root 用户执行的）。

从 Patch 来看的话，is_known_pipename 函数的 pipename 中存在路径符号会有问题：

```
From d2bc9f3afe23ee04d237ae9f4511fbe59a27ff54 Mon Sep 17 00:00:00 2001
From: Volker Lendecke <vl@samba.org>
Date: Mon, 8 May 2017 21:40:40 +0200
Subject: [PATCH] CVE-2017-7494: rpc_server3: Refuse to open pipe names with /
 inside

Bug: https://bugzilla.samba.org/show_bug.cgi?id=12780

Signed-off-by: Volker Lendecke <vl@samba.org>
Reviewed-by: Jeremy Allison <jra@samba.org>
Reviewed-by: Stefan Metzmacher <metze@samba.org>
---
 source3/rpc_server/srv_pipe.c | 5 +++++
 1 file changed, 5 insertions(+)

diff --git a/source3/rpc_server/srv_pipe.c b/source3/rpc_server/srv_pipe.c
index 0633b5f..c3f0cd8 100644
--- a/source3/rpc_server/srv_pipe.c
+++ b/source3/rpc_server/srv_pipe.c
@@ -475,6 +475,11 @@ bool is_known_pipename(const char *pipename, struct ndr_syntax_id *syntax)
 {
 	NTSTATUS status;
 
+	if (strchr(pipename, '/')) {
+		DEBUG(1, ("Refusing open on pipe %s\n", pipename));
+		return false;
+	}
+
 	if (lp_disable_spoolss() && strequal(pipename, "spoolss")) {
 		DEBUG(10, ("refusing spoolss access\n"));
 		return false;
--
1.9.1
```

再延伸下 smb_probe_module 函数中就会形成公告里说的加载攻击者上传的 dll 来任意执行代码了：

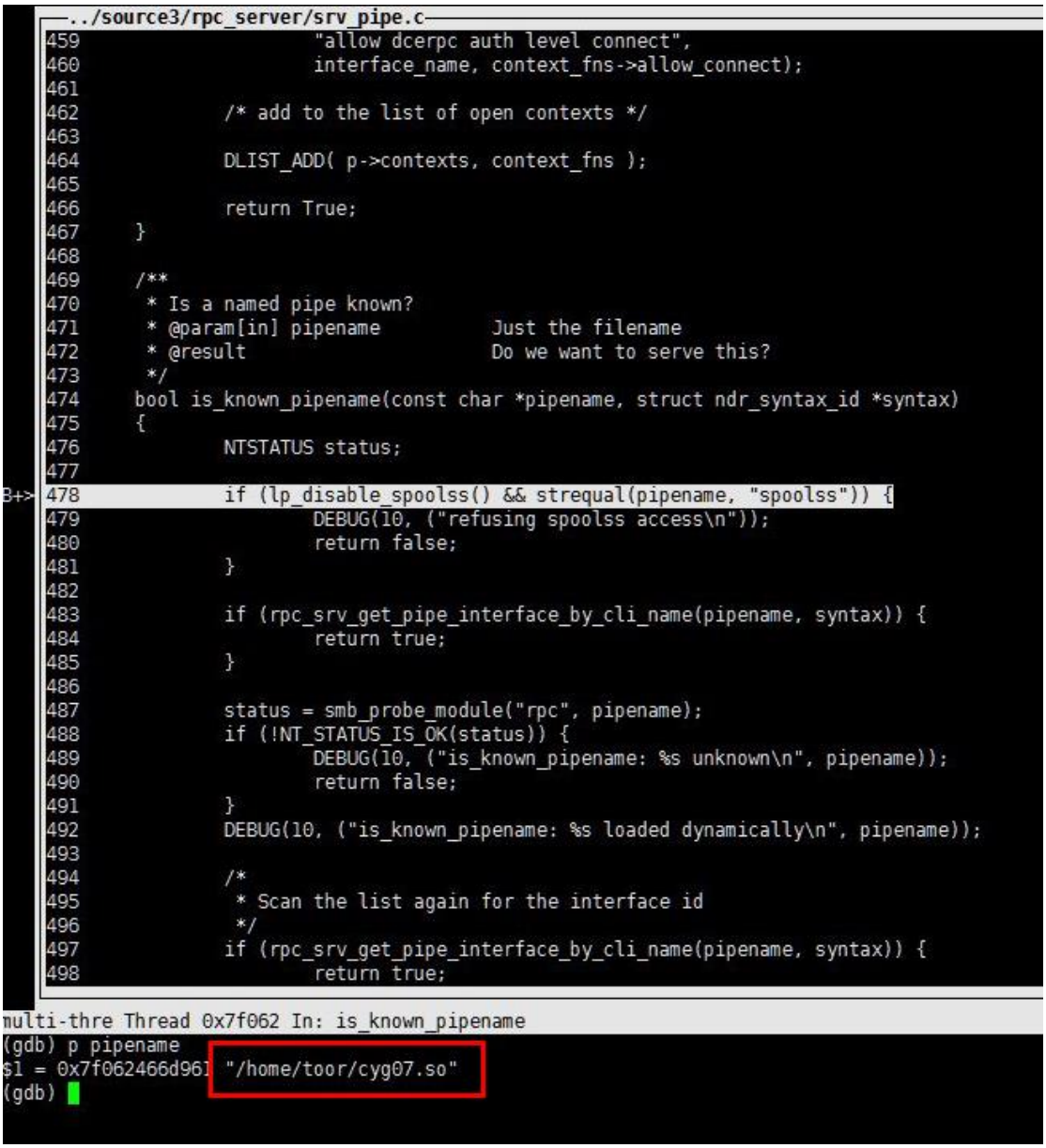
```
bool is_known_pipename(const char *pipename, struct ndr_syntax_id *syntax)
{
    NTSTATUS status;

    if (lp_disable_spoolss() && strequal(pipename, "spoolss")) {
        DEBUG(10, ("refusing spoolss access\n"));
        return false;
    }

    if (rpc_srv_get_pipe_interface_by_cli_name(pipename, syntax)) {
        return true;
    }

    status = smb_probe_module("rpc", pipename);
    if (!NT_STATUS_IS_OK(status)) {
        DEBUG(10, ("is_known_pipename: %s unknown\n", pipename));
        return false;
    }
    DEBUG(10, ("is_known_pipename: %s loaded dynamically\n", pipename));

    /*
     * Scan the list again for the interface id
     */
    if (rpc_srv_get_pipe_interface_by_cli_name(pipename, syntax)) {
        return true;
    }

    DEBUG(10, ("is_known_pipename: pipe %s did not register itself!\n",
           pipename));

    return false;
} ? end is_known_pipename ?
```

4.1 具体攻击过程

1. 构造一个有’/’符号的管道名或路径名，如“/home/toor/cyg07.so”；
2. 通过 smb 的协议主动让服务器 smb 返回该 FID；
3. 后续直接请求这个 FID 就进入上面所说的恶意流程。

4.2 攻击结果

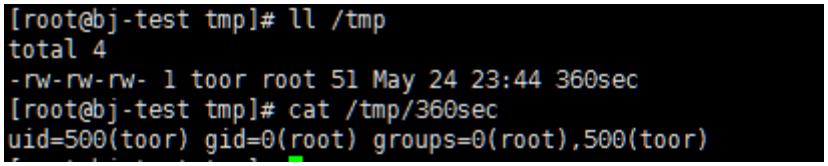
1. 尝试加载 “/home/toor/cyg07.so”恶意 so；



2. 其中 so 代码如下(加载时会调用 samba_init_module 导出函数)

```
#include <stdio.h>
#include <stdlib.h>
int samba_init_module )
{
        printf( "Hi Samba. \nfrom: 360sec" );
        system( "id > /tmp/360sec" );

        return 0;
}
~
~
```

3. 最后我们可以在/tmp/360sec 中看到实际的执行权限(带 root 权限)


[root@bj-test tmp]# ll /tmp
total 4
-rw-rw-rw- 1 toor root 51 May 24 23:44 360sec
[root@bj-test tmp]# cat /tmp/360sec
uid=500(toor) gid=0(root) groups=0(root),500(toor)

第5章 参考文档

详细信息可以参考如下链接：

https://www.samba.org/samba/security/CVE-2017-7494.html

http://m.bobao.360.cn/learning/detail/3900.html?from=timeline&isappinstalled=0