

2019年2月20日，Check Point公布了之前向WinRAR报告的几个安全漏洞，攻击者可利用该漏洞制作恶意ACE格式文件，当该文件被WinRAR解压缩的时候，能利用UNACEV2.dll中的路径遍历漏洞。

WinRAR组件介绍








UNACE.DLL是WinRAR所使用的一个陈旧的动态链接库，用于处理ACE格式的文件，该动态链接库在2006年被编译，没有任何防护措施。

漏洞描述

WinRAR在解压处理ACE格式的文件的過程中存在一处目录穿越漏洞，该漏洞允许解压过程中向任意目录写入文件，利用该漏洞可以向开机启动目录中写入恶意文件导致机器启动时运行恶意文件。










漏洞复现

安装的WinRAR版本

	UnRAR.exe	2017/5/2 1
	WhatsNew.txt	2017/4/13
	WinCon.SFX	2017/5/2 1
	WinRAR.chm	2017/5/2 1
	WinRAR.exe	2017/5/2 1
	Zip.SFX	2017/5/2 1
	zipnew.dat	2019/2/21

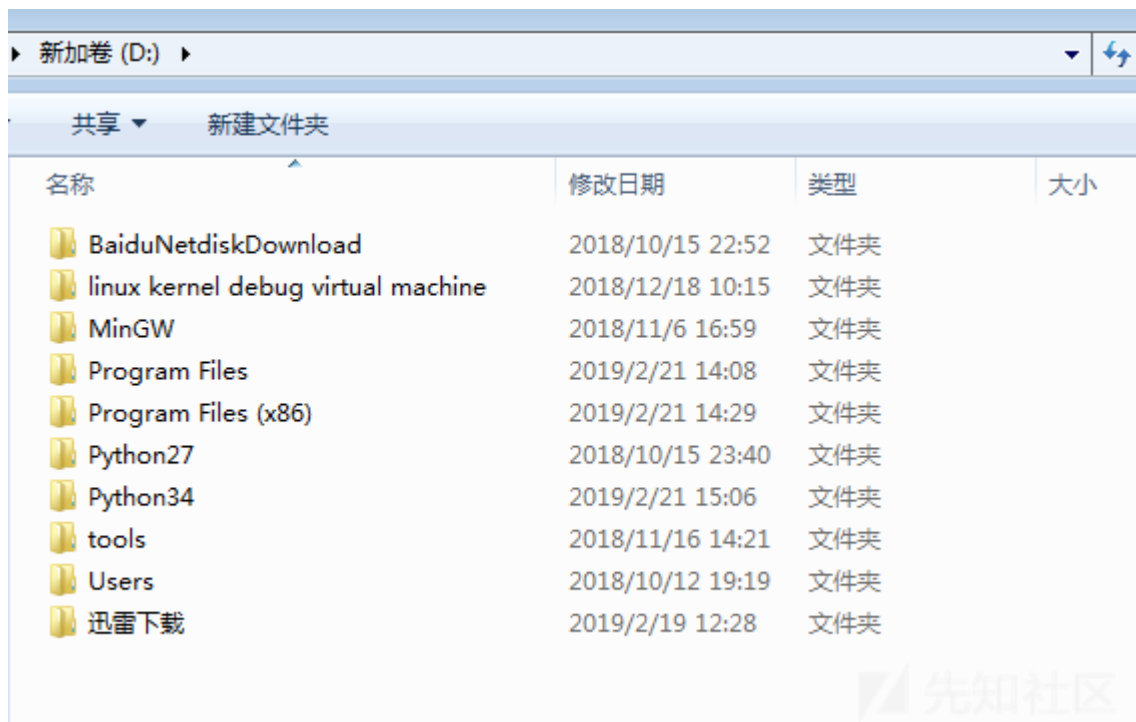
文件说明: WinRAR archiver  
公司: Alexander Roshal  
文件版本: 5.50.1.0  
创建日期: 2019/2/21 14:06  
大小: 1.44 MB

存在漏洞的组件UNACEV2.DLL版本

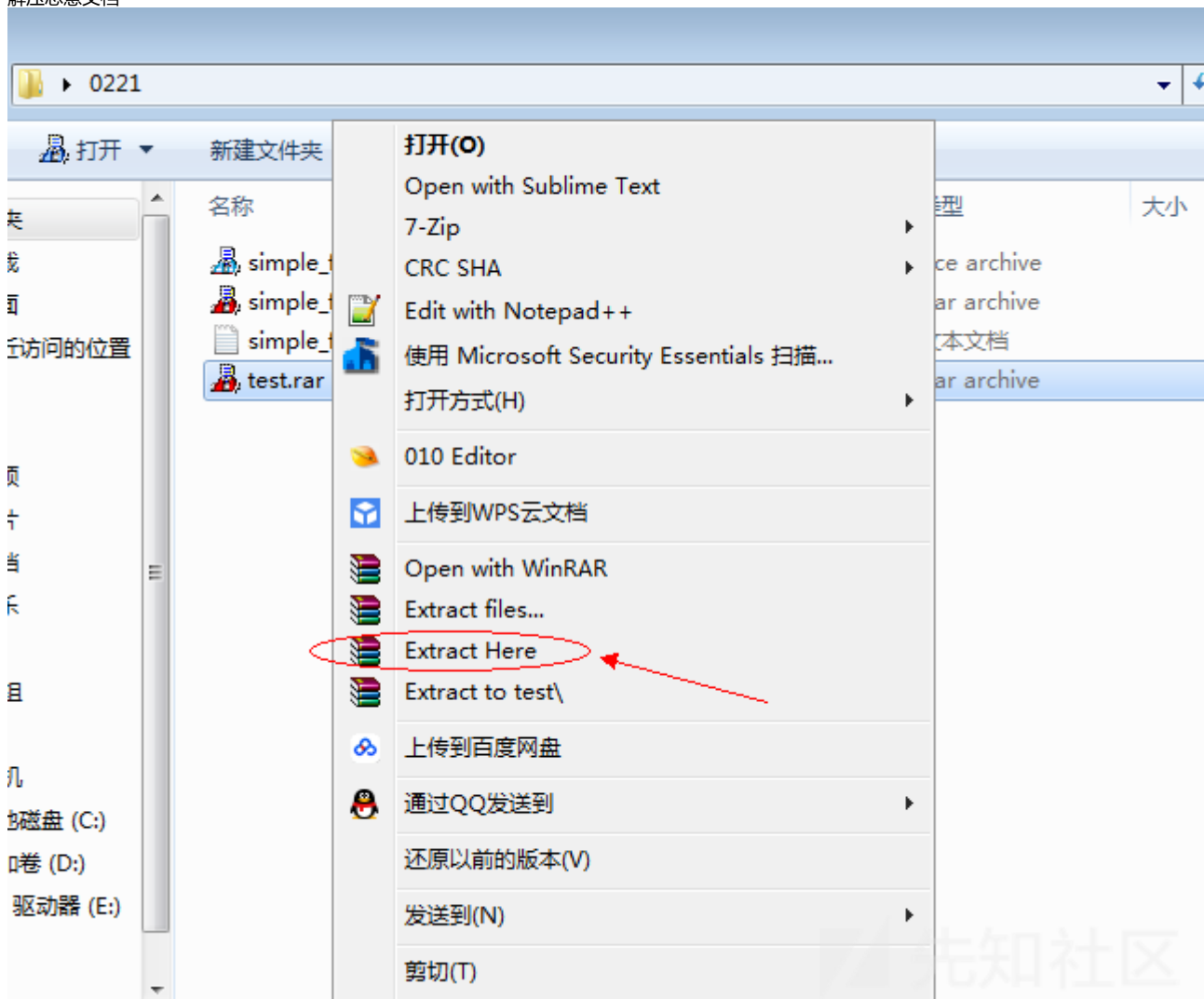
	RarFiles.lst	2017/1/27 1:02
	rarnew.dat	2019/2/21 14:06
	ReadMe.txt	2013/1/11 23:11
	UNACEV2.DLL	2005/8/26 4:50
	Uninstall.exe	2017/5/2 14:03
	Uninstall.lst	2017/5/2 14:04
	UnRAR.exe	2017/5/2 14:03
	WhatsNew.txt	2017/4/13 19:11
	WinCon.SFX	2017/5/2 14:03

文件版本: 2.6.0.0  
创建日期: 2019/2/21 14:06  
大小: 75.5 KB

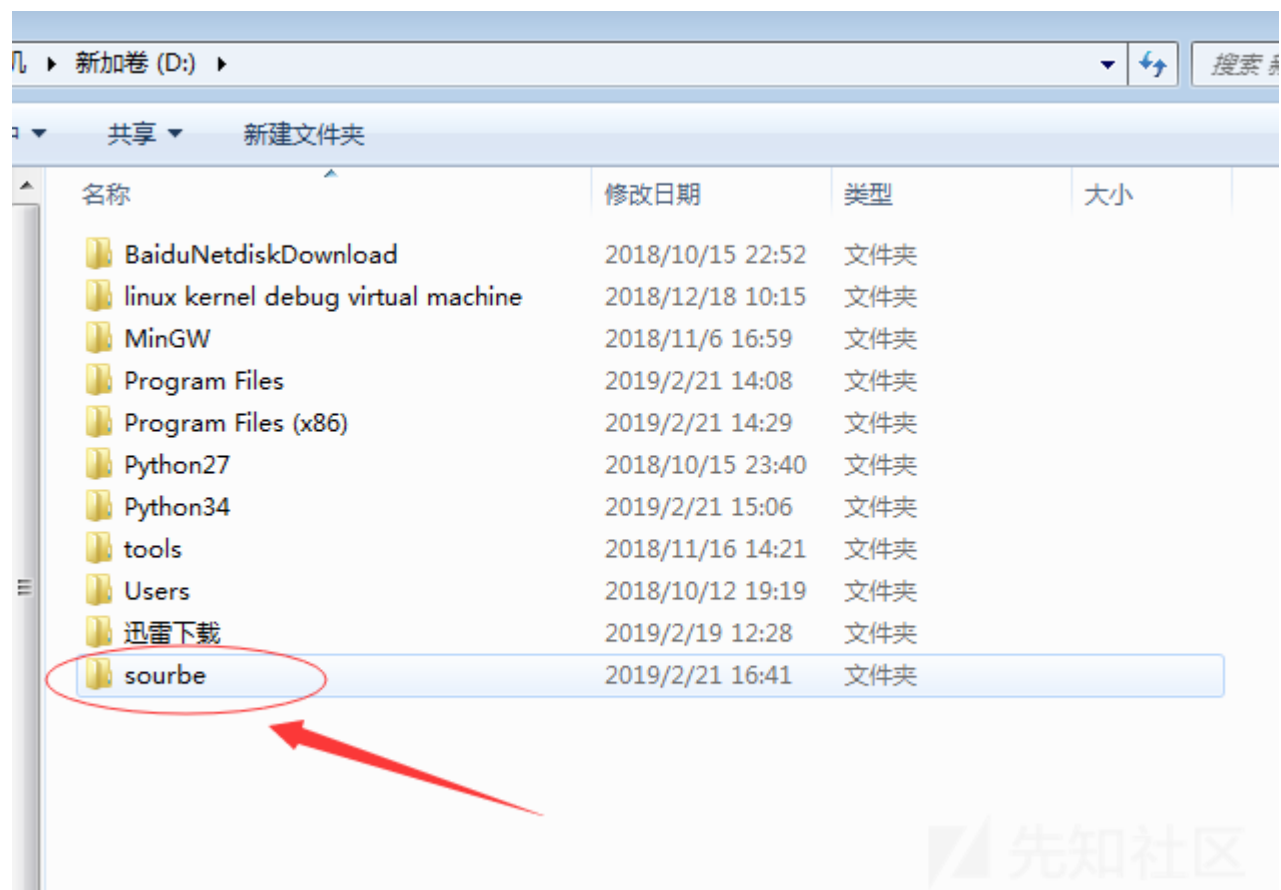
解压恶意ACE文档前的目录结构



解压恶意文档



执行解压缩之后的目录结构



## 影响版本

WinRAR < 5.70 Beta 1

## 修复建议

更新到WinRAR最新版本 5.70 Beta 1

下载地址如下

32位：<http://win-rar.com/fileadmin/winrar-versions/wrar57b1.exe>

64位：<http://win-rar.com/fileadmin/winrar-versions/winrar-x64-57b1.exe>

点击收藏 | 0 关注 | 1

[上一篇：某Server CMS最新6.8....](#) [下一篇：Emotet使用伪造的恶意宏来绕过...](#)

1. 0 条回复

- 动动手指，沙发就是你的了！

[登录](#) 后跟帖

先知社区

[现在登录](#)

热门节点

[技术文章](#)

[社区小黑板](#)

[目录](#)

[RSS](#) [关于社区](#) [友情链接](#) [社区小黑板](#)