山西省互联网网络安全预警信息通报

山西省通信管理局
主办:国家计算机网络应急技术处理协调中心山西分中心　2018 年 2 月 21 日

关于 WinRAR 存在系列远程代码执行漏洞的安全公告

近日,国家信息安全漏洞共享平台(CNVD)收录了 WinRAR 系列任意代码执行漏洞（CNVD-2019-04911、CNVD-2019-04912、CNVD-2019-04913 与 CNVD-2019-04910,分别对应 CVE-2018-20250、CVE-2018-20251、CVE-2018-20252 与 CVE-2018-20253）。攻击者利用上述漏洞，可在未授权的情况下实现任意代码执行。目前，漏洞利用原理已公开，厂商已发布新版本修复此漏洞。

一、漏洞情况分析

WinRAR 是一款功能强大的压缩包管理器，作为档案工具 RAR 在 Windows 环境下的图形界面，可用于备份数据、压缩文件、解压 RAR/ZIP 等格式的文件、创建 RAR/ZIP 等格式的压缩文件，得到了较为广泛的应用。

Check Point 的安全研究团队检测发现 WinRAR 的四个安全漏洞，分别为 ACE 文件验证逻辑绕过漏洞（CVE-2018-20250）、ACE 文件名逻辑验证绕过漏洞（CVE-2018-20251）、ACE/RAR 文件越界写入漏洞（CVE-2018-20252）以及 LHA/LZH 文件越界写入漏洞（CVE-2018-20253。漏洞攻击者利用上述漏洞，通过诱使用户使用 WinRAR 打开恶意构造的压缩包文件，将恶意代码写入系统启动目录或者写入恶意 dll 劫持其他软件进行执行，实现对用户主机的任意代码执行攻击。

CNVD 对上述漏洞的综合评级为“高危”。

二、漏洞影响范围

1、发布时间早于 5.70 Beta 1 版本的 WinRAR 软件;

2、使用 unacev2.dll 动态共享库的解压、文件管理类工具软件。

经腾讯玄武实验室检测发现，除 WinRAR 软件外，共计 38 款软件受此漏洞影响,CNVD 秘书处正通报上述软件厂商，协助其进行漏洞修复，及时消除漏洞攻击隐患。

三、漏洞处置建议

1、使用 WinRAR 软件的用户：WinRAR 厂商已发布新版本修复此漏洞，CNVD 建议立即升级至最新版本:
https://www.win-rar.com/download.html。

2、其他解压、文件管理类软件是否受影响的判断方法：用户可通过检查软件安装目录下是否存在unacev2.dll文件进行判断。

3、建议用户不要打开来历不明的压缩文件。

附：参考链接

https://www.win-rar.com/download.html

https://research.checkpoint.com/extracting-code-execution-from-winrar/