

Blog /

Detecting CVE-2020-0688 Remote Code Execution Vulnerability on Microsoft Exchange Server

February 28, 2020

Detecting CVE-2020-0688 Remote Code Execution Vulnerability on Microsoft Exchange Server

Written by Scott Nusbaum and
Christopher Paschen

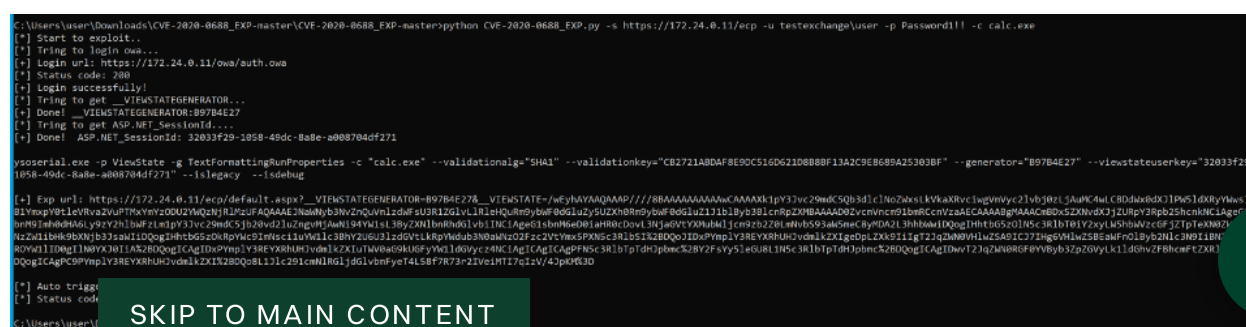
Share



Microsoft recently released a patch for all versions of the Microsoft Exchange server.

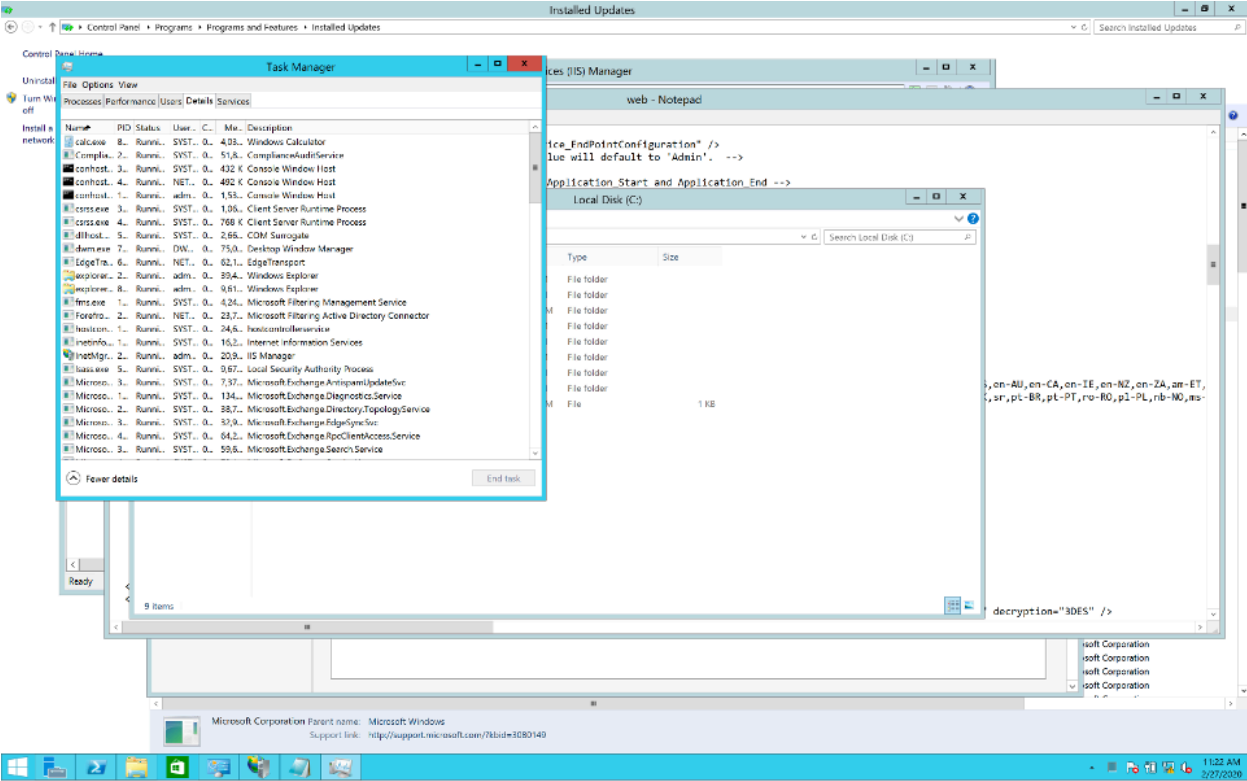
This patch fixes a Remote Code Execution flaw that allows an attacker to send a specially crafted payload to the server and have it execute an embedded command.

Researchers released proof of concept (POC) exploits for this vulnerability on February 24, 2020. The POC exploit tested by TrustedSec was obtained from https://github.com/Yt1g3r/CVE-2020-0688_EXP. TrustedSec's Research Team has verified that these POCs are valid and have gained code execution on internal test systems.

[SKIP TO MAIN CONTENT](#)

An Overview of the Vulnerability

The CVE-2020-0688 vulnerability affects the Exchange Control Panel (ECP) component. The vulnerability affects all installations of Exchange Server because until the most recent patch, all Exchange Servers had the same validation key and validation algorithm in the web.config file. The POC exploits take advantage of same validation key and validation algorithm to craft a serialized __VIEWSTATE request parameter containing an embedded command, signed with the valid key. By default, the POC does not attempt to encrypt the __VIEWSTATE data, although this is an option. The server after, receiving the malicious payload, deserialize the __VIEWSTATE data and execute code as SYSTEM. The image above shows the execution of the POC exploit. The image below shows the Task Manager window where the POC malicious command of calc.exe is executed as SYSTEM.



The exploit first authenticates with the server through a POST /owa/auth.owa request. This POST request contains a valid username and password. After a successful authentication, the exploit requests the /ecp/default.aspx page in an attempt to get the content of __VIEWSTATEGENERATOR and the ASP.NET.SessionID. Using the data obtained from parsing the __VIEWSTATEGNERATOR, the exploit crafts a serialized payload containing the malicious command to be executed. The final serialized payload is then sent back to the /ecp/default.aspx.

The list of pages below are vulnerable to this attack, since the same validation key from the web.config is used in each of the pages, giving the attacker the ability to manipulate the VIEWSTATE. The following is a list of the other pages to be aware of:

- /ecp/default.aspx
- /ecp/PersonalSettings/HomePage.aspx
- /ecp/PersonalSettings/HomePage.aspx4E
- /ecp/Organize/AutomaticReplies.slab
- /ecp/RulesEditor/InboxRules.slab
- /ecp/Organize/DeliveryReports.slab
- /ecp/MyGroups/PersonalGroups.aspx
- /ecp/MyGroups/PersonalGroups.aspx

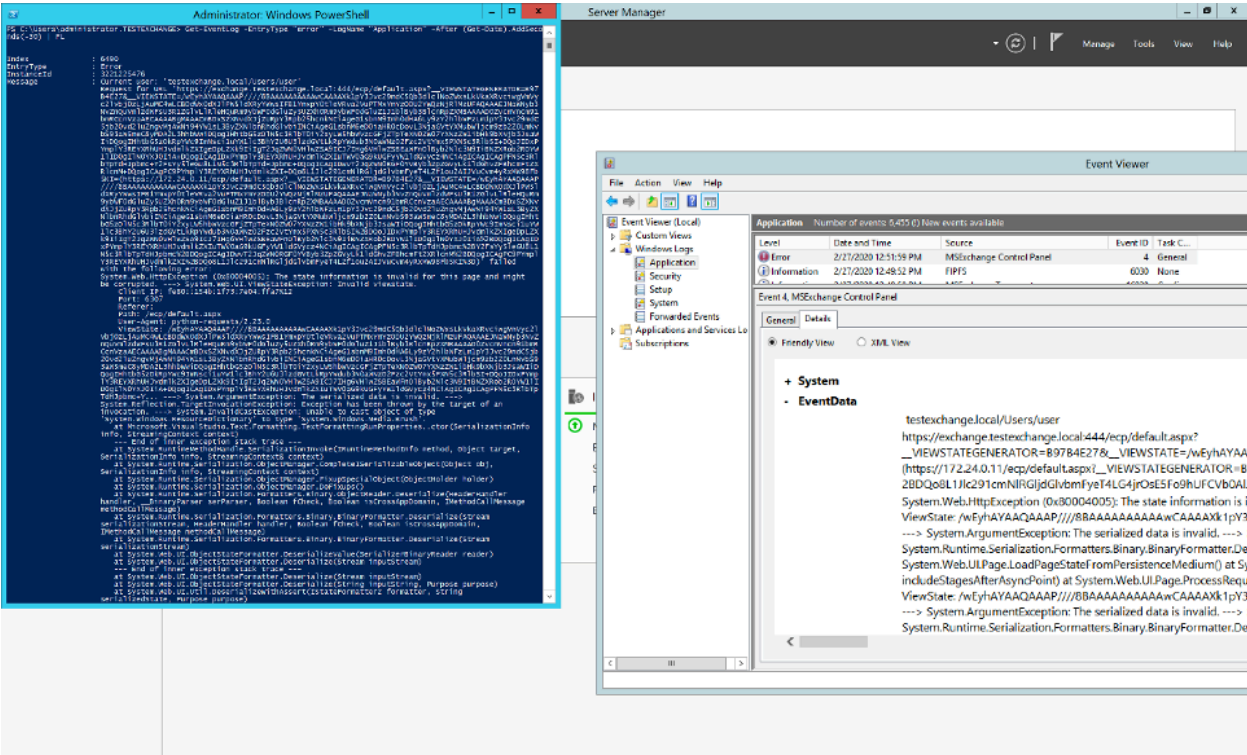
SKIP TO MAIN CONTENT

- /ecp/Customize/Messaging.aspx
- /ecp/Customize/General.aspx
- /ecp/Customize/Calendar.aspx
- /ecp/Customize/SentItems.aspx
- /ecp/PersonalSettings/Password.aspx
- /ecp/SMS/TextMessaging.slab
- /ecp/TroubleShooting/MobileDevices.slab
- /ecp/Customize/Regional.aspx
- /ecp/MyGroups/SearchAllGroups.slab
- /ecp/Security/BlockOrAllow.aspx

Indicators of Compromise

Event Logs

This exploit generates a SYSMON Event ID 4 in the Application logs (shown below). The ERROR message, shown in the Event log, contains the targeted page and includes the serialized payload. Since multiple pages can be targeted, it would be useful to alert on /ecp/ root along with a large __VIEWSTATE variable.



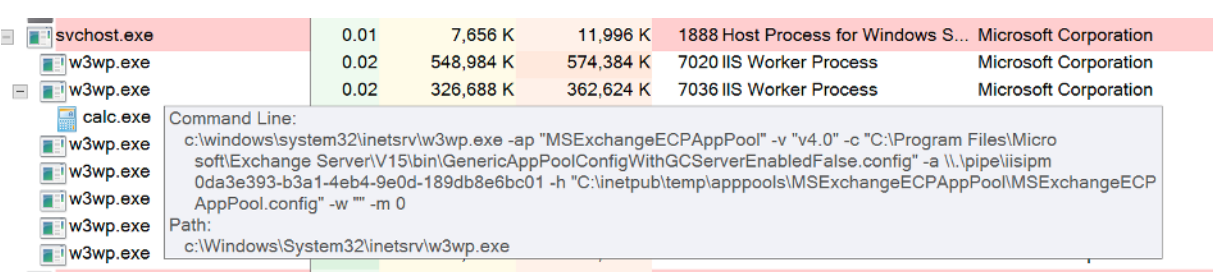
IIS Logs

The following log snippet is an example of the IIS logs after being compromised by the POC. The first indicator is the grouping of requests in the logs, starting with a POST to the /owa/auth.owa, followed by multiple GET requests to one of the targeted URLs listed above, with one of them containing the __VIEWSTATE variable. The __VIEWSTATE should never be sent as part of a GET request. Since this is an automated attack, the timestamps of these requests should be contiguous and tightly grouped within the log. The execution of this POC took less than a second:


```
2020-02-27 16:23:01 172.24.0.11 POST /owa/auth.owa &CorrelationID=;&cafeReqID=
2020-02-27 16:23:01 172.24.0.11 GET /ecp &CorrelationID=;&cafeReqId=bbdc52e
2020-02-27 16:23:01 172.24.0.11 GET /ecp/ &CorrelationID=;&cafeReqId=242a7c
2020-02-27 16:23:01 172.24.0.11 GET /ecp/default.aspx &CorrelationID=;&cafe
2020-02-27 16:23:02 172.24.0.11 GET /ecp/default.aspx __VIEWSTATEGENERATOR=
```

Process Execution

When the exploit sends the payload to the server, the IIS worker process w3wp.exe will spawn the malicious command. The figure below illustrates that the malicious calc.exe is running as a child to the parent w3wp.exe process. The calc.exe is also executed by the SYSTEM user.



Other Logs and Log Locations

The Exchange Server records exceptions under the c:\Program Files\Microsoft\Exchange Server\V15\Logging\ECP\ServerException\ directory. This directory contains the malicious GET requests along with the corresponding query string. The contents of this log file also contain the exception generated when running the POC. The following figure is an example of the content of this log file.

```
00ID=S:URL=https://exchange.testexchange.local:444/ecp/default.aspx?VIEWSTATEGENERATOR=897B4E27&VIEWSTATE=/wEyvwYAAQAAAP////8BAAAAAAAAAAwCAAAAXk1p
00ID=S:URL=https://exchange.testexchange.local:444/ecp/default.aspx?VIEWSTATEGENERATOR=897B4E27&VIEWSTATE=/wEyhATAAQAAAP////8BAAAAAAAAAAwCAAAAXk1p
00ID=S:URL=https://exchange.testexchange.local:444/ecp/default.aspx?VIEWSTATEGENERATOR=897B4E27&VIEWSTATE=/wEyhATAAQAAAP////8BAAAAAAAAAAwCAAAAXk1p
00ID=S:URL=https://exchange.testexchange.local:444/ecp/default.aspx?VIEWSTATEGENERATOR=897B4E27&VIEWSTATE=/wEygYAAQAAAP////8BAAAAAAAAAAwCAAAAXk1p
00ID=S:URL=https://exchange.testexchange.local:444/ecp/default.aspx?VIEWSTATEGENERATOR=897B4E27&VIEWSTATE=/wEyzQYAAQAAAP////8BAAAAAAAAAAwCAAAAXk1p
00ID=S:URL=https://exchange.testexchange.local:444/ecp/default.aspx?VIEWSTATEENCRYPTED=8VIEWSTATE=vzM3rT04ccrU11jfkFHe03eS14tqDxNT+ExINsh7LnhefCF+
00ID=S:URL=https://exchange.testexchange.local:444/ecp/default.aspx?VIEWSTATEENCRYPTED=8VIEWSTATE=qC8X2FQ2VrYFAo8bfpamhVzH7VgDTKs7Nd9p1V14q1N19tD5
00ID=S:URL=https://exchange.testexchange.local:444/ecp/default.aspx?VIEWSTATEENCRYPTED=8VIEWSTATE=H/tY09P4ny6/IkxI1vUGE92z+jIGv6AAwLJ4ooaRt7qBNj12
00ID=S:URL=https://exchange.testexchange.local:444/ecp/default.aspx?VIEWSTATEGENERATOR=897B4E27&VIEWSTATE=/wEyhATAAQAAAP////8BAAAAAAAAAAwCAAAAXk1p
00ID=S:URL=https://exchange.testexchange.local:444/ecp/default.aspx?VIEWSTATEGENERATOR=897B4E27&VIEWSTATE=/wEyhATAAQAAAP////8BAAAAAAAAAAwCAAAAXk1p
00ID=S:URL=https://exchange.testexchange.local:444/ecp/default.aspx?VIEWSTATEGENERATOR=897B4E27&VIEWSTATE=/wEyhATAAQAAAP////8BAAAAAAAAAAwCAAAAXk1p
00ID=S:URL=https://exchange.testexchange.local:444/ecp/default.aspx?VIEWSTATEGENERATOR=897B4E27&VIEWSTATE=/wEyhATAAQAAAP////8BAAAAAAAAAAwCAAAAXk1p
00ID=S:URL=https://exchange.testexchange.local:444/ecp/default.aspx?VIEWSTATEGENERATOR=897B4E27&VIEWSTATE=/wEyhATAAQAAAP////8BAAAAAAAAAAwCAAAAXk1p
00ID=S:URL=https://exchange.testexchange.local:444/ecp/default.aspx?VIEWSTATEGENERATOR=897B4E27&VIEWSTATE=/wEyhATAAQAAAP////8BAAAAAAAAAAwCAAAAXk1p
```

The directory c:\Program Files\Microsoft\Exchange Server\V15\Logging\ECP\Activity\ also contains logs of the connections. These logs differ from those in the ServerException directory in that they contain records for all actions not just the actions that generated exceptions.

Blog

Tools

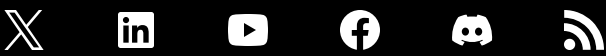
TRUSTEDSEC

3485 Southwestern Boulevard
Fairlawn, OH 44333

SKIP TO MAIN CONTENT

Newsletter Signup

1-877-550-4728



[Terms Of Service](#)

[Privacy Policy](#)

© Copyright 2024 by TrustedSec. All rights reserved.