**CVE 2016-4071**: PHP 5.5.33/7.0.4 - SNMP Format String

**Target:** <http://kpmgspark.com>

* 52.1.175.150
* 52.86.203.217
* 50.16.94.112
* 3.220.228.61
* 3.229.211.71
* 3.215.12.181
* 34.204.135.175
* 52.70.230.150
* 18.233.191.192
* 52.203.87.192

**Note**: additional host seem to be added overtime. This is the most recent DNS recon of the host.

**Host:** Heroku.com

* While Heroku is known for hosting Ruby on rail applications they also offer php and other type of hosting solutions for clients.

**Summary:**

Format string vulnerability in the php\_snmp\_error function in ext/snmp/snmp.c in PHP before 5.5.34, 5.6.x before 5.6.20, and 7.x before 7.0.5 allows remote attackers to execute arbitrary code via format string specifiers in an SNMP::get call.

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4071>

All testing was done from Michael’s own VPS server: 104.237.13.142

In conclusion the host does not look to be vulnerable at the current time to the above vulnerability. It is suggested that we proceed forward with still requesting confirmation from the host on versions of PHP on these assets for further validation.

**Proof of Concept Code:** <https://www.exploit-db.com/exploits/39645>

**Note**: There is not much information on this exploit available on the internet other than the CVE information. Dennis and I searched through multiple channels for additional attack vectors and this is the on the only POC we could find for this vulnerability. W also discovered a Nessus plugin (90631) for testing, however that plugin detects several known issues in those older versions of PHP.

The proof of concept code is written in php and makes use of the SNMP class. The code creates a custom SNMP connection and GET request to carry out the exploit. The exploit it self relies heavily on an exact match of the PHP version that the code was written for. This is due to the ROP chain being written explicitly for the version of PHP that the author wrote it for. To have a proper working exploit one would need to know the exact version of PHP that is installed and that it also had the PHP SNMP class installed as well. Once they know that they could reproduce a working ROP chain and update the POC exploit code accordingly.

**Enumeration:**

Since the exploit relies on SNMP. I first checked each IP address that KPMG Spark is associated with for SNMP. All hosts show that SNMP is filtered and that none of them responded to the request.

**Nmap Enumeration:** The following was ran against each host that is associated with kpmgspark.com. Each host responded the same way. Additional scans redacted for space.

Nmap done: 1 IP address (1 host up) scanned in 1.01 seconds

root@pos:~# nmap -sU --reason -p 161 52.1.175.150

Starting Nmap 7.01 ( [https://nmap.org](https://nmap.org/) ) at 2020-05-21 20:33 UTC

Nmap scan report for [ec2-52-1-175-150.compute-1.amazonaws.com](http://ec2-52-1-175-150.compute-1.amazonaws.com/) (52.1.175.150)

Host is up, received reset ttl 240 (0.032s latency).

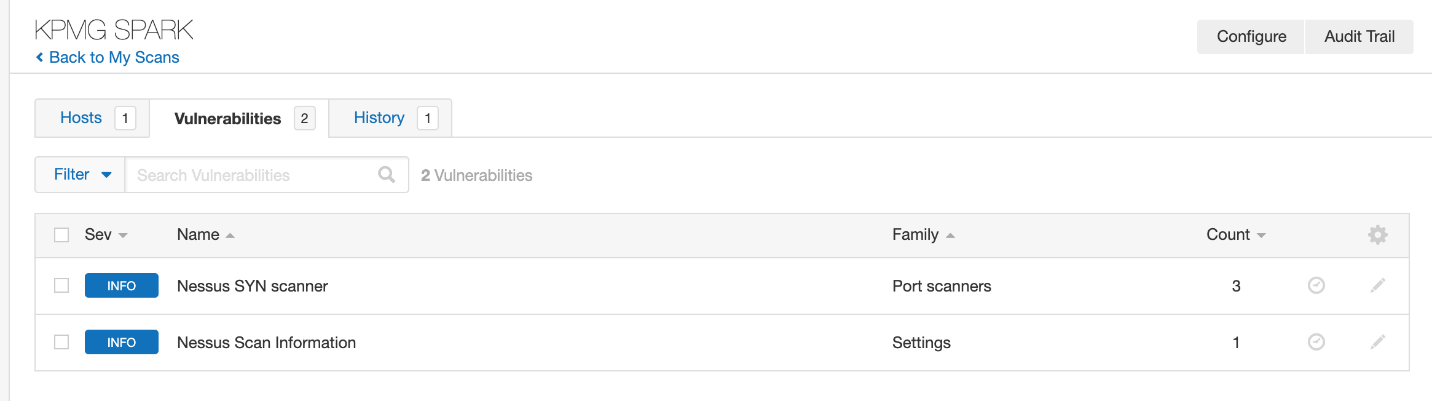
PORT    STATE         SERVICE REASON

161/udp open|filtered snmp    no-response

**Nessus Enumeration:**

Scan Settings:

* Host: kpmgspark.com
* Plugins:
  + CGI Abuse: 90361: PHP 5.6.x < 5.6.20 Multiple Vulnerabilities
  + Web Servers: 48243: PHP Version Detection
* Host came back with no vulnerabilities, though the following ports were detected
  + 21
  + 80
  + 443
* Screenshot:

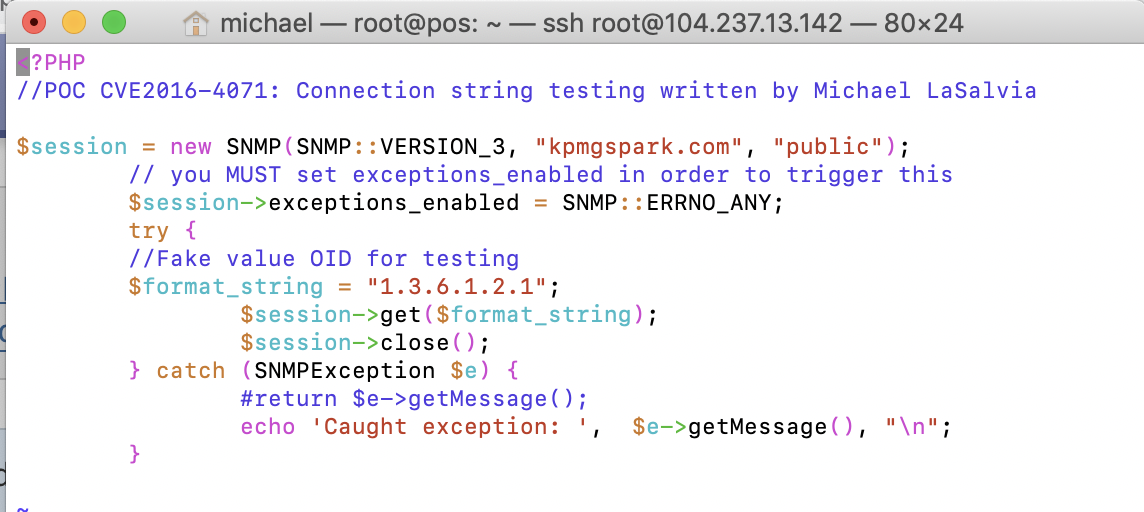


**Proof of Concept Testing:**

The following POC was rewrote in part to fix errors in the running of the code as well as for testing of exploitation. <https://www.exploit-db.com/exploits/39645>

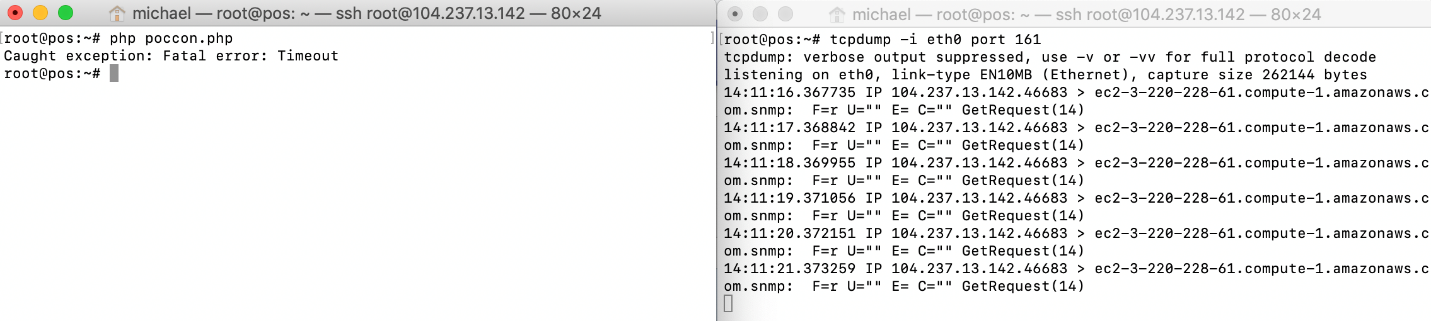
**Modified code:**

See link above for non-modified code.



* Code modified to replace the format\_string payload with a non-malicious string.
* Modified the error connection to show error message to screen.
* If the connection worked, then I would have included the ROP Chain payload, remember ROP requires customization as it is based on the exact matches to bypass ASLR/ DEP /SEH protection.

**Testing POC Code:**

****

* POC ran against kpmgspark.com
* Wire capture shows the request and the GET.
* Error message shows time out which coincides with our previous enumeration from Nessus and NMAP that SNMP is not listening on the hosts associated with the asset in question.