Activity 3.1.1 - CVE Named Vulnerabilities

Name: _____ **Date:** _____ **Class:** _____

Objective : Understand and be able to use the NIST National Vulnerability Database (NVD) to research vulnerabilities.

Background info on named vulnerabilities: The CVE (Common Vulnerability and Exposures) number is the official method of identifying vulnerabilities. However, in 2014 a serious vulnerability was given a name, Heartbleed, for a writeup that was meant to help clarify the risk and methods of mitigation. Since then, it has become a trend to assign fun names to vulnerabilities and some people believe this helps with getting attention to fix those issues.

Instructions: In the NIST NVD database (https://nvd.nist.gov/vuln/search), enter each CVE number in the Advanced Keyword Search (ex. CVE-2014-0160). From the results, determine which of the Named Vulnerabilities below matches with the CVE #. From the NVD description, fill in the table. DO NOT just copy and paste. Simplify the information so that we can easily understand what software or OS is affected and what the attackers will be able to do by taking advantage of this vulnerability. See the Heartbleed example in the first row.

List of Named Vulnerabilities:

Stagefright Badlock Blurtooth Poodle ImageTragick

Name (look in the description for the "aka"	CVE#	Severity V2.0	What does it affect? (Software/app name)	What bad thing can it do?
Ex: HeartBleed	2014-0160	5.0 Medium	OpenSSL 1.0.1	Remote attackers can obtain sensitive info from process memory
1.	2014-3566			
2.	2016-2118			
3.	2015-6602			
4.	2016-3714			
5.	2020-15802			