CMPSCI 177 - Computer Security
Fall 2013
First Homework - Security Terms and Obtaining Vulnerability Information

Due: Wednesday, 9 OCT 13 2:00pm

Part I

Answer questions 1,4, 11, 18, and 21 at the end of Chapter 1 in Bishop's text.

Part II

1. In the past year there have been numerous different Adobe Reader, Acrobat, and Adobe Flash Player vulnerabilities discovered. I would like you to look at the reader and acrobat vulnerabilities discussed in the Adobe Security Advisory APSA13-02. Your task is to find out the details of these vulnerabilities. In particular, what type of vulnerability (i.e., what feature, etc. failed) is each? Also, what applications were affected?

2. Is there a patch for these vulnerabilities?
If yes, who generated the patch? Does it fix all occurrences of the vulnerability identified in question 1, above? If no, why not?

3. What is a "zero-day exploit"? Was there a zero-day exploit of these vulnerabilities? If yes, explain.

Part III

The intent of this part is to get you familiar with the vulnerability databases that are available online.

1. Go to Mitre's **CVE** web site (http://cve.mitre.org).
(a) Use the CVE keyword function to search on the string "Adobe reader and acrobat." How many CVE entries show up with prefix 2013?
(b) What are the corresponding names for the two CVE entries mentioned in APSA13-02?
(c) What is the number of the first vulnerability listed (not necessarily Adobe reader/acrobat related) with a 2013 prefix?
(d) What system(s) was involved in the vulnerability for the first vulnerability listed with a 2013 prefix?

2. Go to NIST's **National Vulnerability Database** (NVD) web site (http://nvd.nist.gov/).
(a) Search for each of the CVE names from part 1(b) above. What are their severity ratings?
(b) When were they published?
(c) Using the statistics section, determine the total number of software SQL Injection vulnerabilities in 2012 and what percentage of the total vulnerabilities in 2012 were SQL Injection?
In case an error occurs, what is the error message?

3. Go to **US-CERT** at web page (http://www.us-cert.gov).
(a) Is there a US-CERT technical alert entry that you can find that refers to either of the CVE names from part 1(b) above?
(b) If yes for part (a), what is the technical alert number?
(c) What is the relationship between US-CERT and the **CERT** coordination center at web page (http://www.cert.org)?
(d) Where is the CERT coordination center physically located?

4. Go to the **Bugtraq** web page (http://www.securityfocus.com)
(a) Can you find any Bugtraq entries that refer to the specific vulnerabilities in APSA13-02?
(b) How does Bugtraq differ from CVE, NVD, CERT, and US-CERT?