Academic Year: Winter Semester 2021/22

6090: Security of Computer and Embedded Systems

Problem Sheet 4

CVSS

In this problem sheet, we will deepen our knowledge in assessing software security risks.

1. Common Vulnerability Scoring System (CVSS)

In this section, you can deepen your understanding of the Common Vulnerability Scoring System (CVSS) in general and, in particular, of assessing the base vectors for CVSS version 3.

Exercise 1: *CVSS (CVE-2015-1098)*

The program iWork in Apple iOS before 8.3 and Apple OS X before 10.10.3 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted iWork file.

What CVSS v3 Base Vector
(AV:[N,A,L,P]/AC:[L,H]/PR:[N,L,H]/UI:[N,R]/S:[U,C]/C:[H,L,N]/I:[H,L,N]/A:[H,L,N])
would you assign to this vulnerability? Provide a brief justification of your assessment.

Exercise 2: *CVSS (CVE-2014-6271)*

GNU Bash through 4.3 processes trailing strings after function definitions in the values of environment variables, which allows remote attackers to execute arbitrary code via a crafted environment, as demonstrated by vectors involving the ForceCommand feature in OpenSSH sshd, the mod_cgi and mod_cgid modules in the Apache HTTP Server, scripts executed by unspecified DHCP clients, and other situations in which setting the environment occurs across a privilege boundary from Bash execution, aka "Shellshock".

What CVSS v3 Base Vector
(AV:[N,A,L,P]/AC:[L,H]/PR:[N,L,H]/UI:[N,R]/S:[U,C]/C:[H,L,N]/I:[H,L,N]/A:[H,L,N])
would you assign to this vulnerability? Provide a brief justification of your assessment.

References

1. Ross J. Anderson. Security Engineering: A Guide to Building Dependable Distributed Systems. John Wiley & Sons, Inc., New York, NY, USA, 1st edition, 2001. The complete book is available at: http://www.cl.cam.ac.uk/~rja14/book.html