Answer to Exercise 1

We can assume that a remote user can create a specially crafted iWork file that, when loaded by the target user (e.g., send via mail or offered as a download), will trigger a memory corruption error and execute arbitrary code. The attacker must deliver and then convince the local user to open the malicious iWork file.

Attack Vector	Local	The vulnerability is in the local parser.
Attack Complexity	Low	Specialised conditions or advanced knowledge is not required.
Privileges Required	Low	
User Interaction	Required	The victim needs to open the malicious iWork file.
Scope	Unchanged	
Confidentiality Impact	High	Arbitrary Code Execution
Integrity Impact	High	Arbitrary Code Execution
Availability Impact	High	Arbitrary Code Execution

Base Score: 7.3 HIGH

Vector: (CVSS:3.1) AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H

Base Score: 6.8 MEDIUM

Vector: (CVSS:2.0) AV:N/AC:M/Au:N /C:P/I:P/A:P

https://nvd.nist.gov/vuln/detail/CVE-2015-1098

Answer to Exercise 2

A successful attack can be launched by an attacker directly against the vulnerable GNU Bash shell, or in certain cases, by an unauthenticated, remote attacker through services either written in GNU Bash or services spawning GNU Bash shells. In the case of an attack against the Apache HTTP Server running dynamic content CGI modules, an attacker can submit a request while providing specially crafted commands as environment variables. These commands will be interpreted by the handler program, the GNU Bash shell, with the privilege of the running HTTPD process. As such, environment variables passed by the attacker could allow installation of software, account enumeration, denial of service, etc. Attacks against other services that have a relationship with the GNU Bash shell are similarly possible.

Attack Vector	Network	Considering the worst case scenario: (web server attack vector).
Attack Complexity	Low	An attacker needs to only gain access to a listening service that uses the GNU Bash shell as an interpreter or interact with a GNU Bash shell directly.
Privileges Required	None	Some attack vectors do not require any privileges (e.g. CGI in web server).
User Interaction	None	No user interaction is required for an attacker to launch a successful attack.
Scope	Unchanged	The vulnerable component is the GNU Bash shell which is used as an interpreter for various services or can be accessed directly, therefore no change in scope occurs during the attack.
Confidentiality Impact	High	Allows an attacker to take complete control of the affected system.
Integrity Impact	High	Allows an attacker to take complete control of the affected system.
Availability Impact	High	Allows an attacker to take complete control of the affected system.

Base Score: 9.8 CRITICAL

Vector: (CVSS:3.1) AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Base Score: 10.0 HIGH

Vector: (CVSS:2.0) AV:N/AC:L/Au:N/C:C/I:C/A:C

https://nvd.nist.gov/vuln/detail/cve-2014-6271

Examples from the Lecture

1) CVE-2013-0375

https://nvd.nist.gov/vuln/detail/CVE-2013-0375

Base Score: 6.4 **MEDIUM**, Vector: **CVSS:3.1** (AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:N)

Base Score: 5.5 **MEDIUM**, Vector: **CVSS:2.0** (AV:N/AC:L/Au:S/C:P/I:P/A:N)

2) CVE-2009-0783

https://nvd.nist.gov/vuln/detail/CVE-2009-0783

Base Score: 4.2 **MEDIUM**, Vector: **CVSS:3.0** (AV:L/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:L)

Base Score: 4.6 **MEDIUM**, Vector: **CVSS:2.0** (AV:L/AC:L/Au:N/C:P/I:P/A:P)

3) CVE-20149253

https://nvd.nist.gov/vuln/detail/CVE-2014-9253

Base Score: 5.4 **MEDIUM**, Vector: **CVSS:3.0** (AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N)

Base Score: 4.3 **MEDIUM**, Vector: **CVSS:2.0** (AV:N/AC:M/Au:N/C:N/I:P/A:N)

A Description on Why CVSS v3.x and v2.0 Scores Differ

(based on the discussion during the lecture)

https://security.stackexchange.com/questions/159290/cvss-score-remote-or-local-scenario

(Explains how the interpretation between these versions are different.)

More Examples with Their Explanations

https://www.first.org/cvss/v3.0/cvss-v30-examples_v1.5.pdf

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