

U2U Online

online.u2u.be/courses/25896/modules/14/24868

Developer and IT Training

U2U

Vulnerable and Outdated Components

OWASP Web Security Threat #6

25°C
Mostly cloudy

Search

6:42 PM
12/29/2023

U2U Online

online.u2u.be/courses/25896/modules/14/24868

Vulnerabilities and Outdated Components

Agenda

- Using Components with known vulnerabilities
- Defenses
- Famous Examples

u2u

25°C Mostly cloudy

Search

6:42 PM 12/29/2023

The image is a screenshot of a web browser displaying a slide from a U2U Online course. The browser's address bar shows the URL `online.u2u.be/courses/25896/modules/14/24868`. The slide itself has a dark blue sidebar on the left with a navigation menu. The main content area is white and features the title **#6: Vulnerable and Outdated Components** in a large, black, sans-serif font. Below the title is a red horizontal line. The slide contains two bullet points, each preceded by a small square icon. The first bullet point is 'Libraries, frameworks and software modules', with a sub-bullet 'Almost always run with full privileges'. The second bullet point is 'Consequences when a component is vulnerable and is exploited', with sub-bullets 'Data loss', 'Server takeover', and '...'. In the top right corner of the slide, there is a black square logo with the white text 'u2u'. The browser's taskbar at the bottom shows the Windows Start button, a search bar, and several application icons. The system tray on the right indicates the temperature is 25°C, the weather is 'Mostly cloudy', and the time is 6:42 PM on 12/29/2023.

U2U Online

online.u2u.be/courses/25896/modules/14/24868

#6: Vulnerable and Outdated Components

- Libraries, frameworks and software modules
 - Almost always run with full privileges
- Consequences when a component is vulnerable and is exploited
 - Data loss
 - Server takeover
 - ...

25°C
Mostly cloudy

6:42 PM
12/29/2023

U2U Online

online.u2u.be/courses/25896/modules/14/24868

Visualizing an Attack

Let's look for vulnerabilities

I'm using VulnerableComponent v1.0

Anything on VulnerableComponent v1.0?

<https://nvd.nist.gov/> - national vulnerability database
<https://cve.mitre.org/> - common vulnerabilities and exposures

vulnerable.website.org

CVE / NVD / others

25°C Mostly cloudy

Search

6:42 PM 12/29/2023

U2U Online

online.u2u.be/courses/25896/modules/14/24868

Vulnerabilities and Outdated Components

Defenses

- Identify the components used
 - Inventory all libraries and components used!
- Monitor the components
 - For CVEs (Common Vulnerabilities and Exposures)
 - For updates
- Keep everything up to date!
- Describe security policies for components usage

25°C Mostly cloudy

6:42 PM 12/29/2023

U2U Online

online.u2u.be/courses/25896/modules/14/24868

Defenses

- Modern tools help detecting vulnerabilities
 - E.g., GitHub
 - E.g., NuGet.org

LanderVe / node-mongo

Code Issues Pull requests Actions Projects Wiki

⚠ We found potential security vulnerabilities in your dependencies.
Only the owner of this repository can see this message.

master 1 branch 0 tags

Microsoft.AspNetCore

Microsoft.AspNetCore.App

⚠ This package has at least one vulnerability with moderate severity. It may lead to specific problems in your project. Try updating the package version.

25°C Mostly cloudy

6:42 PM 12/29/2023

U2U Online

online.u2u.be/courses/25896/modules/14/24868

Defenses

- To detect vulnerabilities in your current project use
 - dotnet list package --vulnerable

Project `CrossSiteScripting` has the following vulnerable packages

Top-level Package	Requested	Resolved	Severity	Advisory URL
> Microsoft.AspNetCore.App	2.1.0	2.1.0	Moderate	https://github.com/advisories/GHSA-cgpw-2g
			Moderate	https://github.com/advisories/GHSA-j378-6m

- npm audit

found 50 vulnerabilities (2 low, 46 moderate, 2 high) in 1322 scanned packages
run `npm audit fix` to fix 42 of them.
7 vulnerabilities require semver-major dependency updates.
1 vulnerability requires manual review. See the full report for details.

25°C Mostly cloudy 6:42 PM 12/29/2023

U2U Online

online.u2u.be/courses/25896/modules/14/24868

Vulnerabilities and Outdated Components

Developer and IT Training

Demo

Using NuGet to keep components up to date

25°C Mostly cloudy

6:42 PM 12/29/2023

The image is a screenshot of a web browser displaying a U2U Online course. The browser's address bar shows the URL `online.u2u.be/courses/25896/modules/14/24868`. The course content is presented on a slide with a dark blue sidebar on the left containing a navigation menu. The slide itself has a white background with a red horizontal line under the title. The title is 'Famous Examples' in a large, black, sans-serif font. In the top right corner of the slide, there is a black square logo with the white text 'u2u'. Below the title, there are two main bullet points, each in red. The first bullet point is 'Heartbleed', followed by two sub-bullets in black: 'A buffer overflow vulnerability in the widely-used encryption library Open SSL' and 'The buffer overflow would return pieces of memory on the server', with the latter having a further sub-bullet: 'Some of which contained confidential information'. The second main bullet point is 'Shellshock', followed by two sub-bullets in black: 'A Shell Command Injection vulnerability in the ubiquitous Bash Unix command line' and 'This vulnerability was there for over 20 years!', with the latter having a further sub-bullet: 'Allows .cgi scripts to be exploited'. At the bottom of the browser window, a Windows taskbar is visible, showing the Start button, a search bar, and several application icons. The system tray on the right shows the date and time as '6:42 PM 12/29/2023'.

U2U Online

online.u2u.be/courses/25896/modules/14/24868

Famous Examples

- **Heartbleed**
 - A buffer overflow vulnerability in the widely-used encryption library Open SSL
 - The buffer overflow would return pieces of memory on the server
 - Some of which contained confidential information
- **Shellshock**
 - A Shell Command Injection vulnerability in the ubiquitous Bash Unix command line
 - This vulnerability was there for over 20 years!
 - Allows .cgi scripts to be exploited

25°C Mostly cloudy

6:42 PM 12/29/2023