Secure Healthcare Software Development

CSP009

PRESENTATION BY: STYLIANOS KARAGIANNIS (PDMFC, PORTUGAL)

Software Security and Health

Introduction to Software Security for Health

Software Security and Health

In this course, we will explore critical aspects of securing healthcare software, including vulnerabilities, cyberattacks, and mitigation strategies.

Critical Assets in Healthcare Domain

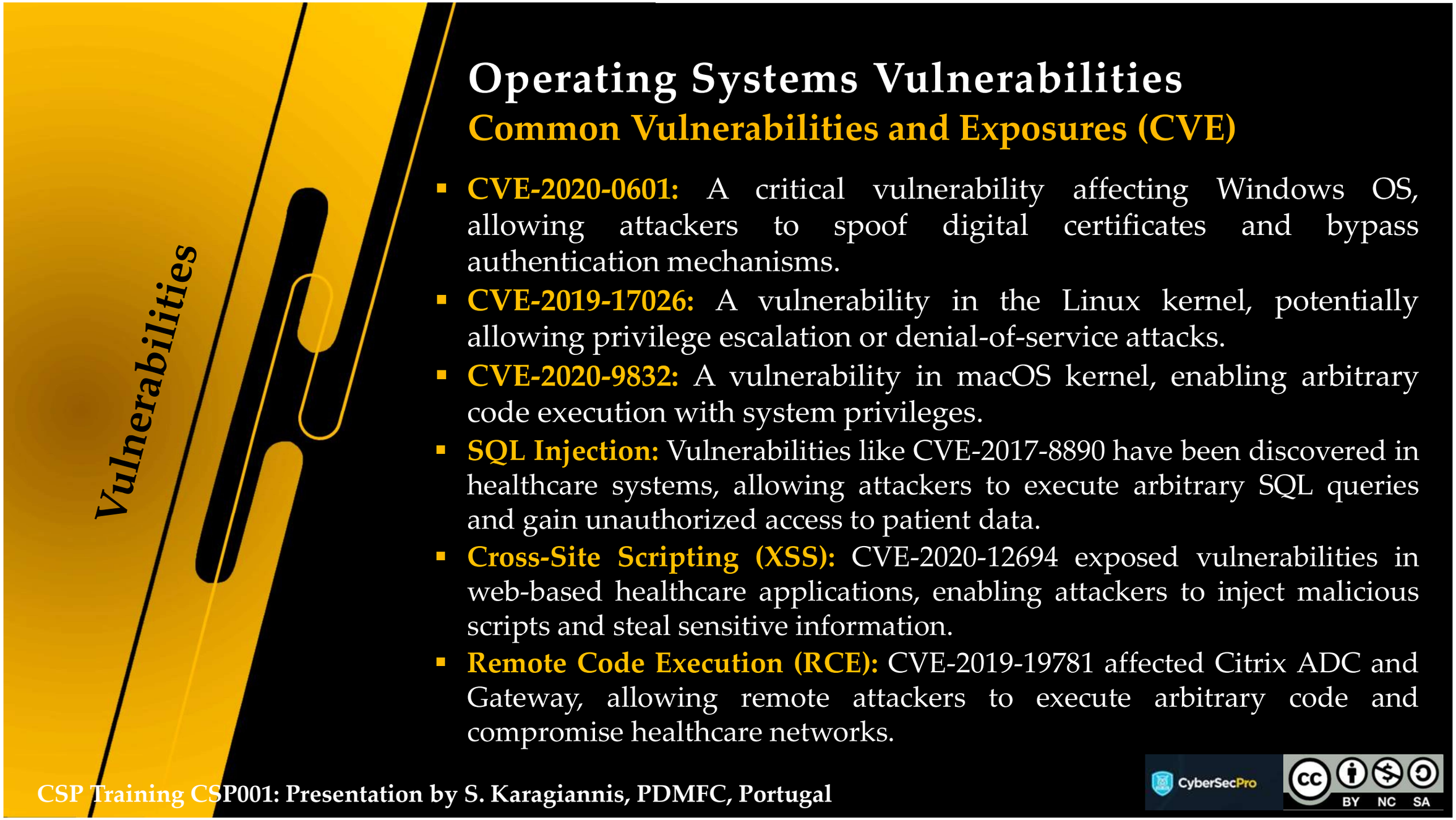
- **Patient Records:** Personally Identifiable Information (PII) and Protected Health Information (PHI) stored in Electronic Health Records (EHR) systems.
- **Medical Devices:** Connected devices such as infusion pumps, pacemakers, and MRI machines that are vulnerable to cyberattacks.
- **Hospital Information Systems (HIS):** Centralized systems for managing patient data, appointments, and billing, like Epic or Cerner.
- **Picture Archiving and Communication System (PACS):** Stores and retrieves medical images such as X-rays and MRIs, like GE Healthcare's Centricity PACS.

Main Cyberattacks in Healthcare

Main Cyberattacks in Healthcare

Ransomware, DoS, Data Breaches, Insider Threats

- **Ransomware Attacks:** Notable incidents include the 2017 WannaCry attack, which affected NHS hospitals, encrypting critical data and demanding ransom for decryption keys.
- **Data Breaches**: In 2015, Anthem Inc. experienced a breach compromising the records of 78.8 million individuals, highlighting the vulnerability of patient data.
- **DDoS Attacks:** Hospitals like the Boston Children's Hospital have faced DDoS attacks leading to service disruption and patient care delays.
- **Insider Threats:** Instances of employees accessing and selling patient data have been reported, emphasizing the need for robust access controls and monitoring.



Operating Systems Vulnerabilities

Common Vulnerabilities and Exposures (CVE)

- **CVE-2020-0601:** A critical vulnerability affecting Windows OS, allowing attackers to spoof digital certificates and bypass authentication mechanisms.
- **CVE-2019-17026:** A vulnerability in the Linux kernel, potentially allowing privilege escalation or denial-of-service attacks.
- **CVE-2020-9832:** A vulnerability in macOS kernel, enabling arbitrary code execution with system privileges.
- **SQL Injection:** Vulnerabilities like CVE-2017-8890 have been discovered in healthcare systems, allowing attackers to execute arbitrary SQL queries and gain unauthorized access to patient data.
- **Cross-Site Scripting (XSS):** CVE-2020-12694 exposed vulnerabilities in web-based healthcare applications, enabling attackers to inject malicious scripts and steal sensitive information.
- **Remote Code Execution (RCE):** CVE-2019-19781 affected Citrix ADC and Gateway, allowing remote attackers to execute arbitrary code and compromise healthcare networks.

Thank you

Presenter: Stylianos Karagiannis (PDMFC, Portugal)

Please send all questions to:
stylianos.karagiannis@pdmfc.com