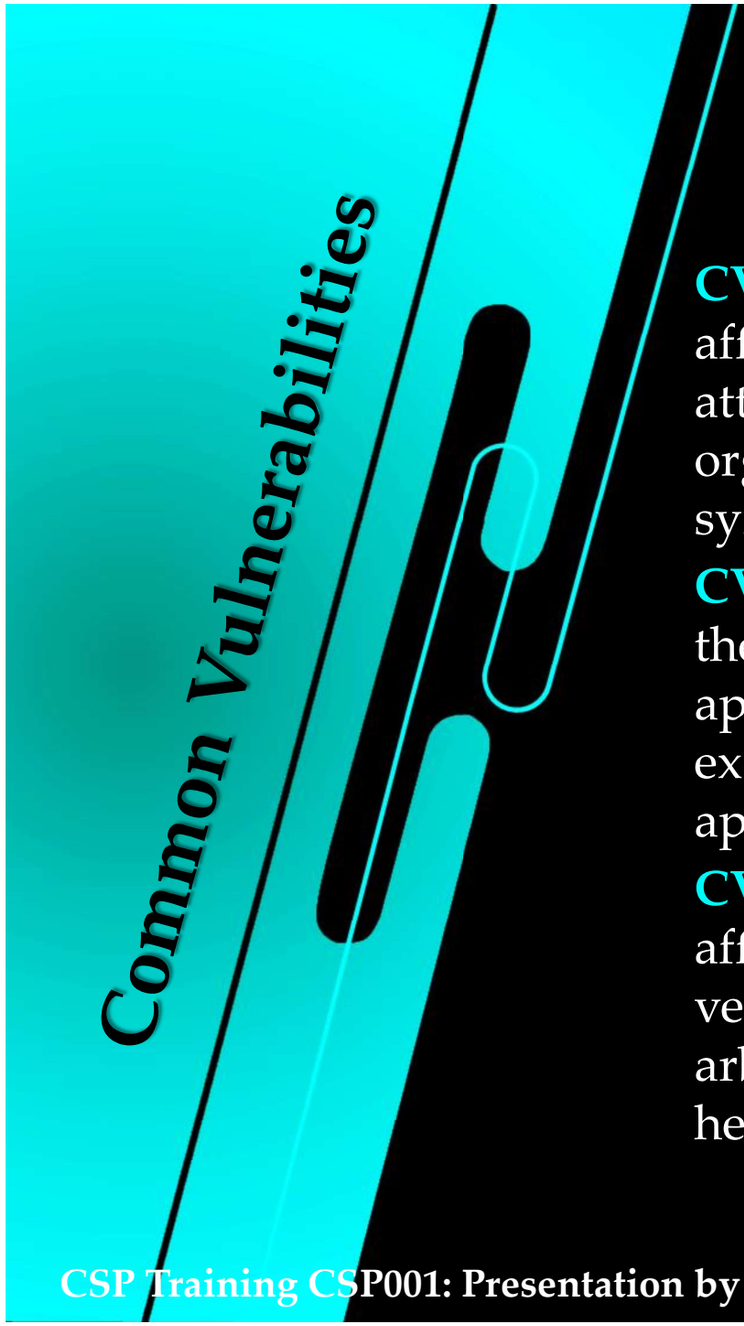
Critical Infrastructure and Security for Health

CSP008

PRESENTATION BY: STYLIANOS KARAGIANNIS (PDMFC, PORTUGAL)



Healthcare Domain

Common Vulnerabilities

CVE-2021-34527: Also known as "PrintNightmare," this vulnerability affects the Windows Print Spooler service, potentially allowing remote attackers to execute arbitrary code with system privileges. Healthcare organizations may be susceptible to exploitation if they use Windows systems for printing medical records or other documents.

CVE-2021-44228: Dubbed "Log4Shell," this critical vulnerability affects the Apache Log4j logging library, commonly used in Java-based applications. Exploitation of this vulnerability could lead to remote code execution, potentially exposing sensitive patient data in healthcare applications that utilize Log4j.

CVE-2019-0708: Commonly referred to as "BlueKeep," this vulnerability affects the Remote Desktop Protocol (RDP) implementation in older versions of Microsoft Windows. If exploited, attackers could execute arbitrary code on vulnerable systems, potentially compromising healthcare networks and systems.

Threat Groups

Healthcare Domain

Threat Groups in Cybersecurity

APT41: APT41 may conduct targeted attacks against healthcare organizations using sophisticated techniques, including spear-phishing emails containing malicious attachments or links designed to exploit vulnerabilities in healthcare systems.

- APT41 targets a hospital's network with spear-phishing emails disguised as legitimate communications from healthcare authorities. The email contains malware that, when opened by unsuspecting staff, compromises the hospital's systems, allowing APT41 to exfiltrate sensitive patient data for espionage or financial gain.

Deep Panda: Deep Panda may exploit vulnerabilities in healthcare systems to gain unauthorized access or conduct espionage activities. They may utilize tactics such as zero-day exploits or supply chain attacks to infiltrate healthcare networks.

- Deep Panda leverages a zero-day vulnerability in a widely used medical device management software installed in hospitals. By exploiting this vulnerability, they gain access to patient records, medical devices, and other sensitive information, which they use for espionage purposes.

Threat Groups Pt.2

Healthcare Domain

Threat Groups in Cybersecurity Pt.2

FIN4: FIN4 may target healthcare employees with sophisticated phishing emails to steal credentials for accessing email and other sensitive information. They may also exploit vulnerabilities in email systems to gain unauthorized access.

- FIN4 sends phishing emails to healthcare executives and financial staff, posing as legitimate requests for financial information or investment opportunities. When recipients unknowingly provide their credentials, FIN4 gains access to confidential financial data, which they use for insider trading or other financial crimes.

menuPass: menuPass may employ various techniques, including social engineering, malware, and remote access tools, to compromise healthcare networks and steal sensitive information.

- menuPass conducts a spear-phishing campaign targeting healthcare researchers working on innovative medical treatments. They trick researchers into downloading malware-infected attachments, which provide menuPass with access to valuable research data, intellectual property, and patient information.

Thank you

Presenter: Stylianos Karagiannis (PDMFC, Portugal)

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