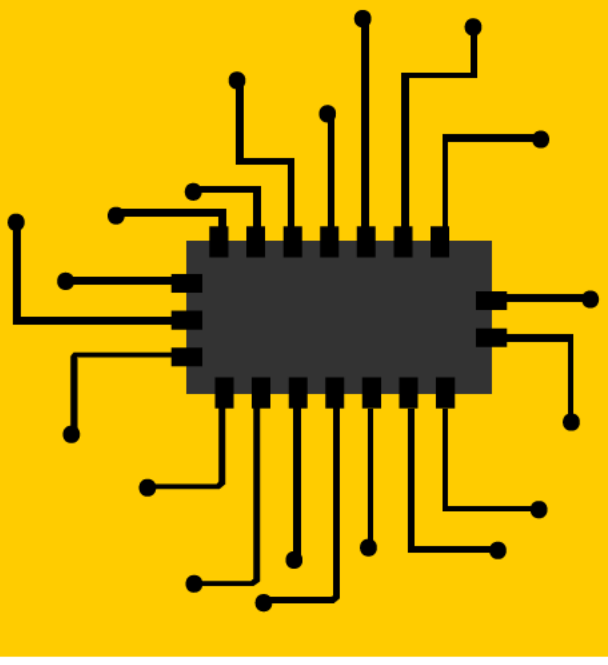

VULNERABLE PROTOCOLS

1 SERVER MESSAGE BLOCK (SMB)

Vulnerability: SMBGhost
Mitigation: Patching all devices immediately per the official Microsoft advisory, Avoiding exposing SMB service discovery to external networks through firewall policies, Using a VPN where remote access is required

2 ADDRESS RESOLUTION PROTOCOL (ARP)

Vulnerability: ARP spoofing attack
Mitigation: Packet filtering, Blocking forged IP addresses, Spoofing detection software

3 HYPERTEXT TRANSFER PROTOCOL (HTTP)

Vulnerability: Browser Reconnaissance and Exfiltration via Adaptive Compression of Hypertext (BREACH)
Mitigation: Using an IPsec virtual private network (VPN), Using an intrusion prevention or intrusion detection system (IPS/IDS), Identifying and updating potentially vulnerable web applications with vulnerability scanner

4 MULTIPURPOSE INTERNET MAIL EXTENSIONS (MIME)

Vulnerability: MIME sniffing
Mitigation: Implementing the use of the 'X-Content-Type-Options: nosniff' HTTP header, Using a separate subdomain to host and deliver all user uploaded content

5 SECURE SOCKETS LAYER (SSL)

Vulnerability: Padding Oracle On Downgraded Legacy Encryption (POODLE)
Mitigation: Upgrading the browser to the latest version, Disabling SSL 3.0 on the server

ESZTER KARAJZ [redacted]