Lab 4.1.1c Vulnerability Scanning (OpenVas)

Thursday, July 20, 2023 6:18 PM

Item:	IP Address:	Rating:	Impact:
CVE-1999-0618 The rexec service is running	172.20.50.53	10.0	rexec (remote execution client for an exec server) has the same kind of functionality that rsh has: you can execute shell commands on a remote computer. Port: 512/tcp
CVE-2020-9761 Java RMI Server Insecure Default Configuration Remote Code Execution Vulnerability	172.20.50.53	10.0	Multiple Java products that implement the RMI Server contain a vulnerability that could allow an unauthenticated, remote attacker to execute arbitrary code on a targeted system with elevated privileges.
CVE-2008-5304/CVE-2008-5305 TWiki XSS and Command Execution Vulnerabilities	172.20.50.53	10.0	The host is running TWiki and is prone to Cross-Site Scripting (XSS) and Command Execution Vulnerabilities.
OS End Of Life Detection	172.20.50.53	10.0	The Operating System on the remote host has reached the end of life and should; not be used anymore.
Possible Backdoor: Ingreslock	172.20.50.53	10.0	Backdoor.Ingreslock is a Trojan that exploits the Ingres database-related vulnerabilities for taking control of your computer. It may launch different attacks but has strong implications in ransomware and file encryption attacks that could hold your files for ransom. Attackers can exploit this issue to execute arbitrary commands in the context of the application. Successful attacks will compromise the affected isystem.
CVE-2011-5330 Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities	172.20.50.53	9.8	Systems using Distributed Ruby (dRuby/DRB), which is available in Ruby versions 1.6 and later, may permit unauthorized systems to execute distributed commands.