Windows Vulnerability Scan Report

System Information

OS: Microsoft Windows 11 Home Single Language
OS Version: 10.0.26100
Architecture: AMD64
.NET Versions: v2.0.50727, v3.0, v3.5, v4, v4.0

Network Information

Open Ports: 4229, 49666, 1462, 28390, 445, 49789, 32682, 49665, 28385, 49667, 9080, 14630, 49664, 49350, 139, 26822, 3306, 49678, 49664, 49670, 3306, 7680, 135, 139, 49668, 7680, 49668, 49666, 135, 49667, 49678, 1462, 4229, 5357, 33060, 24642, 49665, 65001, 445, 5357, 33060, 5040

Potential Vulnerabilities (NVD)

CVE ID	Severity	CVSS	Matched	Description
CVE-2016-10539	HIGH	7.5	Node.js Express framework	negotiator is an HTTP content negotiator for Node.js and is used by many modules and frameworks including Express and Koa. The header for "Accept-Language", when parsed by negotiator 0.6.0 and earlier is vulnerable to Regular Expression Denial of Service via a specially crafted string.
CVE-2021-27434	HIGH	7.5	.NET Framework v3.0	Products with Unified Automation .NET based OPC UA Client/Server SDK Bundle: Versions V3.0.7 and prior (.NET 4.5, 4.0, and 3.5 Framework versions only) are vulnerable to an uncontrolled recursion, which may allow an attacker to trigger a stack overflow.
CVE-2014-6393	MEDIUM	6.1	Node.js Express framework	The Express web framework before 3.11 and 4.x before 4.5 for Node.js does not provide a charset field in HTTP Content-Type headers in 400 level responses, which might allow remote attackers to conduct cross-site scripting (XSS) attacks via characters in a non-standard encoding.
CVE-2024-20994	MEDIUM	5.3	MySQL 8.3.0	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Information Schema). Supported versions that are affected are 8.0.36 and prior and 8.3.0 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromi

CVE-2024-20998	**MEDIUM**	4.9	MySQL 8.3.0	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.36 and prior and 8.3.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL S
CVE-2024-21000	**LOW**	3.8	MySQL 8.3.0	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 8.0.36 and prior and 8.3.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to comprom
CVE-2000-0771	**Unknown**	None	Microsoft Windows RPC	Microsoft Windows 2000 allows local users to cause a denial of service by corrupting the local security policy via malformed RPC traffic, aka the "Local Security Policy Corruption" vulnerability.
CVE-2001-0509	**Unknown**	None	Microsoft Windows RPC	Vulnerabilities in RPC servers in (1) Microsoft Exchange Server 2000 and earlier, (2) Microsoft SQL Server 2000 and earlier, (3) Windows NT 4.0, and (4) Windows 2000 allow remote attackers to cause a denial of service via malformed inputs.
CVE-2002-1140	**Unknown**	None	Microsoft Windows RPC	The Sun Microsystems RPC library Services for Unix 3.0 Interix SD, as implemented on Microsoft Windows NT4, 2000, and XP, allows remote attackers to cause a denial of service (service hang) via malformed packet fragments, aka "Improper parameter size check leading to denial of service."
CVE-2002-0597	**Unknown**	None	microsoft-ds	LANMAN service on Microsoft Windows 2000 allows remote attackers to cause a denial of service (CPU/memory exhaustion) via a stream of malformed data to microsoft-ds port 445.
CVE-1999-1573	**Unknown**	None	unknown	Multiple unknown vulnerabilities in the "r-cmnds" (1) remshd, (2) rexecd, (3) rlogind, (4) rlogin, (5) remsh, (6) rcp, (7) rexec, and (8) rdist for HP-UX 10.00 through 11.00 allow attackers to gain privileges or access files.
CVE-1999-1584	**Unknown**	None	unknown	Unknown vulnerability in (1) loadmodule, and (2) modload if modload is installed with setuid/setgid privileges, in SunOS 4.1.1 through 4.1.3c, and Open Windows 3.0, allows local users to gain root privileges via environment variables, a different vulnerability than CVE-1999-1586.

CVE-1999-1589	**Unknown**	None	unknown	Unspecified vulnerability in crontab in IBM AIX 3.2 allows local users to gain root privileges via unknown attack vectors.