Affected Software	Products Version	Severity	Details of the flaws	Exploitation Status	Vulnerability
Windows	Windows 7, 8.1, RT 8.1, 10, 11 Server 2008 SP2, 2008R2, 2012, 2012 R2, 2016, 2019, 2022 including Server Core Installations Remote Desktop Client	Critical	CVE-2022-21972 CVE-2022-22011 CVE-2022-22012 CVE-2022-22013 CVE-2022-22014 CVE-2022-22015 CVE-2022-22016 CVE-2022-22017 CVE-2022-22019 CVE-2022-22713 CVE-2022-23270 CVE-2022-23279 CVE-2022-24466 CVE-2022-26913 CVE-2022-26923 CVE-2022-26925** CVE-2022-26926 CVE-2022-26927 CVE-2022-26930 CVE-2022-26931 CVE-2022-26932 CVE-2022-26933 CVE-2022-26934 CVE-2022-26935 CVE-2022-26936 CVE-2022-26937 CVE-2022-26938 CVE-2022-26939 CVE-2022-26940 CVE-2022-29102 CVE-2022-29103 CVE-2022-29104 CVE-2022-29105 CVE-2022-29106 CVE-2022-29112 CVE-2022-29113 CVE-2022-29114 CVE-2022-29115 CVE-2022-29116 CVE-2022-29120 CVE-2022-29121 CVE-2022-29122 CVE-2022-29123 CVE-2022-29125 CVE-2022-29126 CVE-2022-29127 CVE-2022-29128 CVE-2022-29129 CVE-2022-29130 CVE-2022-29131 CVE-2022-29132 CVE-2022-29133 CVE-2022-29134 CVE-2022-29135 CVE-2022-29137 CVE-2022-29138 CVE-2022-29139 CVE-2022-29140 CVE-2022-29141 CVE-2022-29142 CVE-2022-29150 CVE-2022-29151	\\\\\\\\	Denial of Service Elevation of Privilege Information Disclosure Remote Code Execution Security Feature Bypass Spoofing
Edge	Chromium-based	Important	CVE-2022-29144 CVE-2022-29146 CVE-2022-29147	Workaround: No Exploited: No Public: No	Elevation of Privilege Spoofing
.NET Framework	2.0 SP2, 3.0 SP2, 3.5, 3.5.1, 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 Core 3.1 .NET 5.0, 6.0	Important	CVE-2022-23267 CVE-2022-29117 CVE-2022-29145 CVE-2022-30130	Workaround: No Exploited: No Public: No	Denial of Service
Visual Studio	2017 15.9 through 15.0 2019 16.11 through 16.0 2022 17.0, 17.1 VS Code	Important	CVE-2022-23267 CVE-2022-29117 CVE-2022-29145 CVE-2022-29148 CVE-2022-30129	Workaround: No Exploited: No Public: No	Denial of Service Remote Code Execution
Office	365 Apps for Enterprise Excel/Word 2013 RT SP1, 2013 SP1, 2016 Publisher 2013 SP1, 2016 Office 2019, Online Server Web Apps Server 2013 SP1 LTSC 2021	Important	CVE-2022-29107 CVE-2022-29109 CVE-2022-29110	Workaround: No Exploited: No Public: No	Remote Code Execution Security Feature Bypass
SharePoint Server	Enterprise Server 2016 Foundation 2013 SP1 Server 2019 Server Enterprise Subscription Edition	Important	CVE-2022-29108	Workaround: No Exploited: No Public: No	Remote Code Execution
Exchange Server	2013 CU23 2016 CU22/23 2019 CU11/12	Important	CVE-2022-21978	Workaround: No Exploited: No Public: No	Elevation of Privilege
Azure	Self-hosted Integration Runtime	Critical	CVE-2022-29972	Workaround: No Exploited: No Public: Yes	Information Disclosure Remote Code Execution