奇安信集团 2024 年 07 月补丁库

更新通告

第一次更新

奇安信集团漏洞补丁运营团队

2024 年 07 月 10 日

目 录

文档信息

文档名称	奇安信集团 2024 年 07 月补丁库更新通告		
文档编号	Qi An Xin Group-MSPatch-2024-0701		
发布日期	2024-07-10	密级	公开
关键字	Microsoft、漏洞、补丁		
发布团队	奇安信集团漏洞补丁运营团队		

第1章 安全通告

尊敬的客户：

奇安信集团最新补丁库(V6版本:2024.07.10.1,V10版本:2024.07.10.1000)已发布，本次更新推送了29个微软安全补丁，修复了94个安全漏洞，其中5个微软官方评级为“严重(Critical)”，89个评级为“重要(Important)”，这些漏洞影响Windows、Office等产品。

第2章 重点关注补丁

本月有 20 个安全漏洞经奇安信评估满足以下任一条件，需要重点关注。

1. 漏洞等级（Severity）=严重（Critical），
2. 公开披露（Publicly Disclosed）=是（Yes），
3. 已受攻击（Exploited）=是（Yes），
4. 漏洞的可利用性（Exploitability Assessment）="已被利用（Exploitation Detected）" 或 "很可能被利用（Exploitation More Likely）"

详情如下：

KBID	修复的漏洞	漏洞的影响	漏洞等级	公开披露	已受攻击	漏洞的可利用性
5040434	CVE-2024-38076	Remote Code Execution	Critical	No	No	Exploitation Less Likely
5040430						
5040437						
5040434	CVE-2024-38085	Elevation of Privilege	Important	No	No	Exploitation More Likely
5040490						
5040499						
5040456						
5040485						
5040430						
5040427						
5040448						
5040497						
5040498						
5040437						
5040431						
5040442						
5040434	CVE-2024-38077	Remote Code Execution	Critical	No	No	Exploitation Less Likely
5040490						
5040499						
5040456						
5040485						
5040430						
5040497						
5040498						
5040437						
5040434	CVE-2024-38052	Elevation of Privilege	Important	No	No	Exploitation More Likely
5040490						
5040499						

5040456						
5040485						
5040430						
5040427						
5040448						
5040497						
5040498						
5040437						
5040431						
5040442						
5040434	CVE-2024-38112	Spoofing	Important	No	Yes	Exploitation Detected
5040490						
5040426						
5040499						
5040456						
5040430						
5040427						
5040448						
5040437						
5040431						
5040442						
5040434	CVE-2024-38079	Elevation of Privilege	Important	No	No	Exploitation More Likely
5040490						
5040499						
5040456						
5040485						
5040430						
5040427						
5040448						
5040497						
5040498						
5040437						
5040431						
5040442						
5040434	CVE-2024-38060	Remote Code Execution	Critical	No	No	Exploitation More Likely
5040456						
5040485						
5040430						
5040427						
5040448						
5040497						

5040498						
5040437						
5040431						
5040442						
5040434	CVE-2024-38066	Elevation of Privilege	Important	No	No	Exploitation More Likely
5040490						
5040499						
5040456						
5040485						
5040430						
5040427						
5040448						
5040497						
5040498						
5040434	CVE-2024-38054	Elevation of Privilege	Important	No	No	Exploitation More Likely
5040490						
5040499						
5040456						
5040485						
5040430						
5040427						
5040448						
5040497						
5040498						
5040437						
5040431						
5040442						
5040434	CVE-2024-38099	Denial of Service	Important	No	No	Exploitation More Likely
5040490						
5040499						
5040456						
5040485						
5040430						
5040497						
5040498						
5040437						
5040434	CVE-2024-38100	Elevation of Privilege	Important	No	No	Exploitation More Likely
5040430						
5040437						
5040434	CVE-2024-38074	Remote Code Execution	Critical	No	No	Exploitation Less Likely
5040456						

5040485						
5040430						
5040497						
5040498						
5040437						
5040434	CVE-2024-39684	Elevation of Privilege	Moderate	No	No	Exploitation More Likely
5040490						
5040499						
5040456						
5040485						
5040430						
5040427						
5040448						
5040497						
5040498						
5040437						
5040431						
5040442						
5040427	CVE-2024-38059	Elevation of Privilege	Important	No	No	Exploitation More Likely
5040437						
5040431						
5040442						
5002618	CVE-2024-38024	Remote Code Execution	Important	No	No	Exploitation More Likely
5002618	CVE-2024-38023	Remote Code Execution	Critical	No	No	Exploitation More Likely
5002618	CVE-2024-38094	Remote Code Execution	Important	No	No	Exploitation More Likely
5040437	CVE-2024-38080	Elevation of Privilege	Important	No	Yes	Exploitation Detected
5040431						
5040442						
5002620	CVE-2024-38021	Remote Code Execution	Important	No	No	Exploitation More Likely
5040442	CVE-2024-37985	Information Disclosure	Important	Yes	No	Exploitation Less Likely

第3章 已知问题和特殊调整

本月暂无已知问题和特殊调整。

第4章 漏洞补丁详细列表

本月微软发布的系统安全更新补丁共 13 个，详细列表如下：

KBID	奇安信集团级别	补丁名称	CVE 漏洞	漏洞的影响	漏洞等级	公开披露	已受攻击	漏洞的可利用性
5040434	高危	July 9, 2024—KB5040434 (OS Build 14393.7159) - Microsoft Support for Windows 10, version 1607, all editions, Windows Server 2016, all editions	CVE-2024-35270	Denial of Service	Important	No	No	2
			CVE-2024-28899	Security Feature Bypass	Important	No	No	2
			CVE-2024-38043	Elevation of Privilege	Important	No	No	2
			CVE-2024-38104	Remote Code Execution	Important	No	No	2
			CVE-2024-38031	Denial of Service	Important	No	No	2
			CVE-2024-37969	Security Feature Bypass	Important	No	No	2
			CVE-2024-38076	Remote Code Execution	Critical	No	No	2
			CVE-2024-38033	Elevation of Privilege	Important	No	No	2
			CVE-2024-38070	Security Feature Bypass	Important	No	No	2
			CVE-2024-38085	Elevation of Privilege	Important	No	No	1
			CVE-2024-38049	Remote Code Execution	Important	No	No	2
			CVE-2024-38077	Remote Code Execution	Critical	No	No	2
			CVE-2024-37971	Security Feature Bypass	Important	No	No	2
			CVE-2024-37974	Security Feature Bypass	Important	No	No	2
			CVE-2024-38011	Security Feature Bypass	Important	No	No	2

			CVE-2024-37987	Security Feature Bypass	Important	No	No	2
			CVE-2024-30079	Elevation of Privilege	Important	No	No	2
			CVE-2024-38027	Denial of Service	Important	No	No	2
			CVE-2024-37973	Security Feature Bypass	Important	No	No	2
			CVE-2024-38057	Elevation of Privilege	Important	No	No	2
			CVE-2024-30013	Remote Code Execution	Important	No	No	2
			CVE-2024-38052	Elevation of Privilege	Important	No	No	1
			CVE-2024-37972	Security Feature Bypass	Important	No	No	2
			CVE-2024-38053	Remote Code Execution	Important	No	No	2
			CVE-2024-38112	Spoofing	Important	No	Yes	0
			CVE-2024-30071	Information Disclosure	Important	No	No	2
			CVE-2024-37988	Security Feature Bypass	Important	No	No	2
			CVE-2024-38030	Spoofing	Important	No	No	2
			CVE-2024-38047	Elevation of Privilege	Important	No	No	2
			CVE-2024-38019	Remote Code Execution	Important	No	No	2
			CVE-2024-38055	Information Disclosure	Important	No	No	2
			CVE-2024-30081	Spoofing	Important	No	No	2
			CVE-2024-37986	Security Feature Bypass	Important	No	No	2
			CVE-2024-38517	Elevation of Privilege	Moderate	No	No	2
			CVE-2024-37975	Security Feature Bypass	Important	No	No	2
			CVE-2024-38073	Denial of Service	Important	No	No	2
			CVE-2024-38058	Security Feature Bypass	Important	No	No	2

			CVE-2024-38017	Information Disclosure	Important	No	No	2
			CVE-2024-3596	Spoofing	Important	No	No	2
			CVE-2024-38079	Elevation of Privilege	Important	No	No	1
			CVE-2024-38062	Elevation of Privilege	Important	No	No	2
			CVE-2024-38056	Information Disclosure	Important	No	No	2
			CVE-2024-38060	Remote Code Execution	Critical	No	No	1
			CVE-2024-38066	Elevation of Privilege	Important	No	No	1
			CVE-2024-37989	Security Feature Bypass	Important	No	No	2
			CVE-2024-38101	Denial of Service	Important	No	No	2
			CVE-2024-38051	Remote Code Execution	Important	No	No	2
			CVE-2024-38091	Denial of Service	Important	No	No	2
			CVE-2024-38044	Remote Code Execution	Important	No	No	2
			CVE-2024-38068	Denial of Service	Important	No	No	2
			CVE-2024-38022	Elevation of Privilege	Important	No	No	2
			CVE-2024-38013	Elevation of Privilege	Important	No	No	2
			CVE-2024-38065	Security Feature Bypass	Important	No	No	2
			CVE-2024-38054	Elevation of Privilege	Important	No	No	1
			CVE-2024-38069	Security Feature Bypass	Important	No	No	2
			CVE-2024-38034	Elevation of Privilege	Important	No	No	2
			CVE-2024-38105	Denial of Service	Important	No	No	2
			CVE-2024-38048	Denial of Service	Important	No	No	2

			CVE-2024-38025	Remote Code Execution	Important	No	No	2
			CVE-2024-38072	Denial of Service	Important	No	No	2
			CVE-2024-38061	Elevation of Privilege	Important	No	No	2
			CVE-2024-38081	Elevation of Privilege	Important	No	No	2
			CVE-2024-38102	Denial of Service	Important	No	No	2
			CVE-2024-38071	Denial of Service	Important	No	No	2
			CVE-2024-38064	Information Disclosure	Important	No	No	2
			CVE-2024-38099	Denial of Service	Important	No	No	1
			CVE-2024-38041	Information Disclosure	Important	No	No	2
			CVE-2024-38100	Elevation of Privilege	Important	No	No	1
			CVE-2024-37984	Security Feature Bypass	Important	No	No	2
			CVE-2024-30098	Security Feature Bypass	Important	No	No	2
			CVE-2024-38010	Security Feature Bypass	Important	No	No	2
			CVE-2024-38050	Elevation of Privilege	Important	No	No	2
			CVE-2024-38074	Remote Code Execution	Critical	No	No	2
			CVE-2024-38067	Denial of Service	Important	No	No	2
			CVE-2024-38028	Remote Code Execution	Important	No	No	2
			CVE-2024-38015	Denial of Service	Important	No	No	2
			CVE-2024-37970	Security Feature Bypass	Important	No	No	2
			CVE-2024-39684	Elevation of Privilege	Moderate	No	No	1

5040490	高危	July 9, 2024—KB5040490 (Security-only update) - Microsoft Support for Windows Server 2008 Datacenter ESU,Windows Server 2008 Standard ESU,Windows Server 2008 Enterprise ESU	CVE-2024-38079	Elevation of Privilege	Important	No	No	1
			CVE-2024-35270	Denial of Service	Important	No	No	2
			CVE-2024-38052	Elevation of Privilege	Important	No	No	1
			CVE-2024-38066	Elevation of Privilege	Important	No	No	1
			CVE-2024-38112	Spoofing	Important	No	Yes	0
			CVE-2024-38051	Remote Code Execution	Important	No	No	2
			CVE-2024-38091	Denial of Service	Important	No	No	2
			CVE-2024-38044	Remote Code Execution	Important	No	No	2
			CVE-2024-38071	Denial of Service	Important	No	No	2
			CVE-2024-38064	Information Disclosure	Important	No	No	2
			CVE-2024-38068	Denial of Service	Important	No	No	2
			CVE-2024-38099	Denial of Service	Important	No	No	1
			CVE-2024-38019	Remote Code Execution	Important	No	No	2
			CVE-2024-38104	Remote Code Execution	Important	No	No	2
			CVE-2024-38054	Elevation of Privilege	Important	No	No	1
			CVE-2024-38031	Denial of Service	Important	No	No	2
			CVE-2024-38055	Information Disclosure	Important	No	No	2
			CVE-2024-30081	Spoofing	Important	No	No	2
			CVE-2024-38085	Elevation of Privilege	Important	No	No	1
			CVE-2024-38049	Remote Code Execution	Important	No	No	2
			CVE-2024-38048	Denial of Service	Important	No	No	2

			CVE-2024-38077	Remote Code Execution	Critical	No	No	2
			CVE-2024-38073	Denial of Service	Important	No	No	2
			CVE-2024-38067	Denial of Service	Important	No	No	2
			CVE-2024-38028	Remote Code Execution	Important	No	No	2
			CVE-2024-38017	Information Disclosure	Important	No	No	2
			CVE-2024-38027	Denial of Service	Important	No	No	2
			CVE-2024-3596	Spoofing	Important	No	No	2
			CVE-2024-38025	Remote Code Execution	Important	No	No	2
			CVE-2024-38057	Elevation of Privilege	Important	No	No	2
			CVE-2024-39684	Elevation of Privilege	Moderate	No	No	1
5040499	高危	July 9, 2024—KB5040499 (Monthly Rollup) - Microsoft Support for Windows Server 2008 Datacenter ESU,Windows Server 2008 Standard ESU,Windows Server 2008	CVE-2024-38079	Elevation of Privilege	Important	No	No	1
			CVE-2024-35270	Denial of Service	Important	No	No	2
			CVE-2024-38052	Elevation of Privilege	Important	No	No	1
			CVE-2024-38066	Elevation of Privilege	Important	No	No	1
			CVE-2024-38112	Spoofing	Important	No	Yes	0
			CVE-2024-38051	Remote Code Execution	Important	No	No	2
			CVE-2024-38091	Denial of Service	Important	No	No	2
			CVE-2024-38044	Remote Code Execution	Important	No	No	2
			CVE-2024-38071	Denial of Service	Important	No	No	2
			CVE-2024-38064	Information Disclosure	Important	No	No	2
			CVE-2024-38068	Denial of Service	Important	No	No	2

		Enterprise ESU	CVE-2024-38099	Denial of Service	Important	No	No	1
			CVE-2024-38019	Remote Code Execution	Important	No	No	2
			CVE-2024-38104	Remote Code Execution	Important	No	No	2
			CVE-2024-38054	Elevation of Privilege	Important	No	No	1
			CVE-2024-38031	Denial of Service	Important	No	No	2
			CVE-2024-38055	Information Disclosure	Important	No	No	2
			CVE-2024-30081	Spoofing	Important	No	No	2
			CVE-2024-38085	Elevation of Privilege	Important	No	No	1
			CVE-2024-38049	Remote Code Execution	Important	No	No	2
			CVE-2024-38048	Denial of Service	Important	No	No	2
			CVE-2024-38077	Remote Code Execution	Critical	No	No	2
			CVE-2024-38073	Denial of Service	Important	No	No	2
			CVE-2024-38067	Denial of Service	Important	No	No	2
			CVE-2024-38028	Remote Code Execution	Important	No	No	2
			CVE-2024-38017	Information Disclosure	Important	No	No	2
			CVE-2024-38027	Denial of Service	Important	No	No	2
			CVE-2024-3596	Spoofing	Important	No	No	2
			CVE-2024-38025	Remote Code Execution	Important	No	No	2
			CVE-2024-38057	Elevation of Privilege	Important	No	No	2
			CVE-2024-39684	Elevation of Privilege	Moderate	No	No	1
5040456	高危	July 9, 2024—	CVE-2024-38079	Elevation of Privilege	Important	No	No	1

		KB5040456 (Monthly Rollup) - Microsoft Support for Windows Server 2012 R2 ESU	CVE-2024-35270	Denial of Service	Important	No	No	2
			CVE-2024-38102	Denial of Service	Important	No	No	2
			CVE-2024-38052	Elevation of Privilege	Important	No	No	1
			CVE-2024-37972	Security Feature Bypass	Important	No	No	2
			CVE-2024-38056	Information Disclosure	Important	No	No	2
			CVE-2024-38060	Remote Code Execution	Critical	No	No	1
			CVE-2024-38066	Elevation of Privilege	Important	No	No	1
			CVE-2024-38053	Remote Code Execution	Important	No	No	2
			CVE-2024-37989	Security Feature Bypass	Important	No	No	2
			CVE-2024-38101	Denial of Service	Important	No	No	2
			CVE-2024-38112	Spoofing	Important	No	Yes	0
			CVE-2024-38051	Remote Code Execution	Important	No	No	2
			CVE-2024-28899	Security Feature Bypass	Important	No	No	2
			CVE-2024-38091	Denial of Service	Important	No	No	2
			CVE-2024-38044	Remote Code Execution	Important	No	No	2
			CVE-2024-30071	Information Disclosure	Important	No	No	2
			CVE-2024-38071	Denial of Service	Important	No	No	2
			CVE-2024-37988	Security Feature Bypass	Important	No	No	2
			CVE-2024-38068	Denial of Service	Important	No	No	2
			CVE-2024-38064	Information Disclosure	Important	No	No	2
			CVE-2024-38022	Elevation of Privilege	Important	No	No	2

			CVE-2024-38013	Elevation of Privilege	Important	No	No	2
			CVE-2024-38065	Security Feature Bypass	Important	No	No	2
			CVE-2024-37987	Security Feature Bypass	Important	No	No	2
			CVE-2024-38030	Spoofing	Important	No	No	2
			CVE-2024-38099	Denial of Service	Important	No	No	1
			CVE-2024-38019	Remote Code Execution	Important	No	No	2
			CVE-2024-37974	Security Feature Bypass	Important	No	No	2
			CVE-2024-38104	Remote Code Execution	Important	No	No	2
			CVE-2024-38054	Elevation of Privilege	Important	No	No	1
			CVE-2024-38031	Denial of Service	Important	No	No	2
			CVE-2024-37984	Security Feature Bypass	Important	No	No	2
			CVE-2024-30098	Security Feature Bypass	Important	No	No	2
			CVE-2024-38010	Security Feature Bypass	Important	No	No	2
			CVE-2024-38055	Information Disclosure	Important	No	No	2
			CVE-2024-38034	Elevation of Privilege	Important	No	No	2
			CVE-2024-37969	Security Feature Bypass	Important	No	No	2
			CVE-2024-30081	Spoofing	Important	No	No	2
			CVE-2024-38033	Elevation of Privilege	Important	No	No	2
			CVE-2024-38105	Denial of Service	Important	No	No	2
			CVE-2024-38070	Security Feature Bypass	Important	No	No	2
			CVE-2024-38085	Elevation of Privilege	Important	No	No	1

			CVE-2024-38050	Elevation of Privilege	Important	No	No	2
			CVE-2024-38049	Remote Code Execution	Important	No	No	2
			CVE-2024-38048	Denial of Service	Important	No	No	2
			CVE-2024-37986	Security Feature Bypass	Important	No	No	2
			CVE-2024-38077	Remote Code Execution	Critical	No	No	2
			CVE-2024-38074	Remote Code Execution	Critical	No	No	2
			CVE-2024-37971	Security Feature Bypass	Important	No	No	2
			CVE-2024-38011	Security Feature Bypass	Important	No	No	2
			CVE-2024-38067	Denial of Service	Important	No	No	2
			CVE-2024-38073	Denial of Service	Important	No	No	2
			CVE-2024-38028	Remote Code Execution	Important	No	No	2
			CVE-2024-38058	Security Feature Bypass	Important	No	No	2
			CVE-2024-37975	Security Feature Bypass	Important	No	No	2
			CVE-2024-38017	Information Disclosure	Important	No	No	2
			CVE-2024-38027	Denial of Service	Important	No	No	2
			CVE-2024-37973	Security Feature Bypass	Important	No	No	2
			CVE-2024-3596	Spoofing	Important	No	No	2
			CVE-2024-30079	Elevation of Privilege	Important	No	No	2
			CVE-2024-38025	Remote Code Execution	Important	No	No	2
			CVE-2024-38057	Elevation of Privilege	Important	No	No	2
			CVE-2024-38015	Denial of Service	Important	No	No	2

			CVE-2024-37970	Security Feature Bypass	Important	No	No	2
			CVE-2024-38061	Elevation of Privilege	Important	No	No	2
			CVE-2024-39684	Elevation of Privilege	Moderate	No	No	1
5040485	高危	July 9, 2024—KB5040485 (Monthly Rollup) - Microsoft Support for Windows Server 2012 ESU	CVE-2024-38079	Elevation of Privilege	Important	No	No	1
			CVE-2024-35270	Denial of Service	Important	No	No	2
			CVE-2024-38102	Denial of Service	Important	No	No	2
			CVE-2024-38052	Elevation of Privilege	Important	No	No	1
			CVE-2024-37972	Security Feature Bypass	Important	No	No	2
			CVE-2024-38060	Remote Code Execution	Critical	No	No	1
			CVE-2024-38066	Elevation of Privilege	Important	No	No	1
			CVE-2024-38053	Remote Code Execution	Important	No	No	2
			CVE-2024-37989	Security Feature Bypass	Important	No	No	2
			CVE-2024-38101	Denial of Service	Important	No	No	2
			CVE-2024-28899	Security Feature Bypass	Important	No	No	2
			CVE-2024-38051	Remote Code Execution	Important	No	No	2
			CVE-2024-38091	Denial of Service	Important	No	No	2
			CVE-2024-38044	Remote Code Execution	Important	No	No	2
			CVE-2024-38071	Denial of Service	Important	No	No	2
			CVE-2024-37988	Security Feature Bypass	Important	No	No	2
			CVE-2024-38068	Denial of Service	Important	No	No	2

			CVE-2024-38064	Information Disclosure	Important	No	No	2
			CVE-2024-38022	Elevation of Privilege	Important	No	No	2
			CVE-2024-38013	Elevation of Privilege	Important	No	No	2
			CVE-2024-38030	Spoofing	Important	No	No	2
			CVE-2024-38099	Denial of Service	Important	No	No	1
			CVE-2024-38019	Remote Code Execution	Important	No	No	2
			CVE-2024-37974	Security Feature Bypass	Important	No	No	2
			CVE-2024-38104	Remote Code Execution	Important	No	No	2
			CVE-2024-38054	Elevation of Privilege	Important	No	No	1
			CVE-2024-38031	Denial of Service	Important	No	No	2
			CVE-2024-37984	Security Feature Bypass	Important	No	No	2
			CVE-2024-38010	Security Feature Bypass	Important	No	No	2
			CVE-2024-38055	Information Disclosure	Important	No	No	2
			CVE-2024-38034	Elevation of Privilege	Important	No	No	2
			CVE-2024-37969	Security Feature Bypass	Important	No	No	2
			CVE-2024-30081	Spoofing	Important	No	No	2
			CVE-2024-38033	Elevation of Privilege	Important	No	No	2
			CVE-2024-38105	Denial of Service	Important	No	No	2
			CVE-2024-38070	Security Feature Bypass	Important	No	No	2
			CVE-2024-38085	Elevation of Privilege	Important	No	No	1
			CVE-2024-38049	Remote Code Execution	Important	No	No	2

			CVE-2024-38050	Elevation of Privilege	Important	No	No	2
			CVE-2024-38048	Denial of Service	Important	No	No	2
			CVE-2024-37986	Security Feature Bypass	Important	No	No	2
			CVE-2024-38077	Remote Code Execution	Critical	No	No	2
			CVE-2024-38074	Remote Code Execution	Critical	No	No	2
			CVE-2024-37971	Security Feature Bypass	Important	No	No	2
			CVE-2024-38011	Security Feature Bypass	Important	No	No	2
			CVE-2024-38073	Denial of Service	Important	No	No	2
			CVE-2024-38067	Denial of Service	Important	No	No	2
			CVE-2024-38028	Remote Code Execution	Important	No	No	2
			CVE-2024-38058	Security Feature Bypass	Important	No	No	2
			CVE-2024-37975	Security Feature Bypass	Important	No	No	2
			CVE-2024-38017	Information Disclosure	Important	No	No	2
			CVE-2024-38027	Denial of Service	Important	No	No	2
			CVE-2024-37973	Security Feature Bypass	Important	No	No	2
			CVE-2024-3596	Spoofing	Important	No	No	2
			CVE-2024-37987	Security Feature Bypass	Important	No	No	2
			CVE-2024-38025	Remote Code Execution	Important	No	No	2
			CVE-2024-38057	Elevation of Privilege	Important	No	No	2
			CVE-2024-38015	Denial of Service	Important	No	No	2
			CVE-2024-37970	Security Feature Bypass	Important	No	No	2

			CVE-2024-38061	Elevation of Privilege	Important	No	No	2
			CVE-2024-39684	Elevation of Privilege	Moderate	No	No	1
5040430	高危	July 9, 2024—KB5040430 (OS Build 17763.6054) - Microsoft Support for Win 10 Ent LTSC 2019,Win 10 IoT Ent LTSC 2019,Windows 10 IoT Core 2019 LTSC,Windows Server 2019	CVE-2024-35270	Denial of Service	Important	No	No	2
			CVE-2024-28899	Security Feature Bypass	Important	No	No	2
			CVE-2024-38043	Elevation of Privilege	Important	No	No	2
			CVE-2024-38104	Remote Code Execution	Important	No	No	2
			CVE-2024-38031	Denial of Service	Important	No	No	2
			CVE-2024-37969	Security Feature Bypass	Important	No	No	2
			CVE-2024-38076	Remote Code Execution	Critical	No	No	2
			CVE-2024-38033	Elevation of Privilege	Important	No	No	2
			CVE-2024-38070	Security Feature Bypass	Important	No	No	2
			CVE-2024-38085	Elevation of Privilege	Important	No	No	1
			CVE-2024-38049	Remote Code Execution	Important	No	No	2
			CVE-2024-38077	Remote Code Execution	Critical	No	No	2
			CVE-2024-37971	Security Feature Bypass	Important	No	No	2
			CVE-2024-37974	Security Feature Bypass	Important	No	No	2
			CVE-2024-38011	Security Feature Bypass	Important	No	No	2
			CVE-2024-37987	Security Feature Bypass	Important	No	No	2
			CVE-2024-30079	Elevation of Privilege	Important	No	No	2
			CVE-2024-38027	Denial of Service	Important	No	No	2

			CVE-2024-37973	Security Feature Bypass	Important	No	No	2
			CVE-2024-38057	Elevation of Privilege	Important	No	No	2
			CVE-2024-30013	Remote Code Execution	Important	No	No	2
			CVE-2024-38052	Elevation of Privilege	Important	No	No	1
			CVE-2024-37972	Security Feature Bypass	Important	No	No	2
			CVE-2024-38053	Remote Code Execution	Important	No	No	2
			CVE-2024-38112	Spoofing	Important	No	Yes	0
			CVE-2024-30071	Information Disclosure	Important	No	No	2
			CVE-2024-37988	Security Feature Bypass	Important	No	No	2
			CVE-2024-38030	Spoofing	Important	No	No	2
			CVE-2024-38047	Elevation of Privilege	Important	No	No	2
			CVE-2024-38019	Remote Code Execution	Important	No	No	2
			CVE-2024-38055	Information Disclosure	Important	No	No	2
			CVE-2024-30081	Spoofing	Important	No	No	2
			CVE-2024-37986	Security Feature Bypass	Important	No	No	2
			CVE-2024-38517	Elevation of Privilege	Moderate	No	No	2
			CVE-2024-21417	Elevation of Privilege	Important	No	No	2
			CVE-2024-37975	Security Feature Bypass	Important	No	No	2
			CVE-2024-38058	Security Feature Bypass	Important	No	No	2
			CVE-2024-38073	Denial of Service	Important	No	No	2
			CVE-2024-38017	Information Disclosure	Important	No	No	2
			CVE-2024-3596	Spoofing	Important	No	No	2

			CVE-2024-38079	Elevation of Privilege	Important	No	No	1
			CVE-2024-38062	Elevation of Privilege	Important	No	No	2
			CVE-2024-38056	Information Disclosure	Important	No	No	2
			CVE-2024-38060	Remote Code Execution	Critical	No	No	1
			CVE-2024-38066	Elevation of Privilege	Important	No	No	1
			CVE-2024-37989	Security Feature Bypass	Important	No	No	2
			CVE-2024-38101	Denial of Service	Important	No	No	2
			CVE-2024-38051	Remote Code Execution	Important	No	No	2
			CVE-2024-38091	Denial of Service	Important	No	No	2
			CVE-2024-38044	Remote Code Execution	Important	No	No	2
			CVE-2024-37981	Security Feature Bypass	Important	No	No	2
			CVE-2024-38068	Denial of Service	Important	No	No	2
			CVE-2024-38022	Elevation of Privilege	Important	No	No	2
			CVE-2024-38013	Elevation of Privilege	Important	No	No	2
			CVE-2024-38065	Security Feature Bypass	Important	No	No	2
			CVE-2024-38054	Elevation of Privilege	Important	No	No	1
			CVE-2024-38069	Security Feature Bypass	Important	No	No	2
			CVE-2024-38034	Elevation of Privilege	Important	No	No	2
			CVE-2024-38105	Denial of Service	Important	No	No	2
			CVE-2024-38048	Denial of Service	Important	No	No	2

			CVE-2024-38025	Remote Code Execution	Important	No	No	2
			CVE-2024-38072	Denial of Service	Important	No	No	2
			CVE-2024-38061	Elevation of Privilege	Important	No	No	2
			CVE-2024-38102	Denial of Service	Important	No	No	2
			CVE-2024-38071	Denial of Service	Important	No	No	2
			CVE-2024-38064	Information Disclosure	Important	No	No	2
			CVE-2024-38099	Denial of Service	Important	No	No	1
			CVE-2024-38041	Information Disclosure	Important	No	No	2
			CVE-2024-38100	Elevation of Privilege	Important	No	No	1
			CVE-2024-37984	Security Feature Bypass	Important	No	No	2
			CVE-2024-30098	Security Feature Bypass	Important	No	No	2
			CVE-2024-38010	Security Feature Bypass	Important	No	No	2
			CVE-2024-38050	Elevation of Privilege	Important	No	No	2
			CVE-2024-38074	Remote Code Execution	Critical	No	No	2
			CVE-2024-38067	Denial of Service	Important	No	No	2
			CVE-2024-38028	Remote Code Execution	Important	No	No	2
			CVE-2024-38015	Denial of Service	Important	No	No	2
			CVE-2024-37970	Security Feature Bypass	Important	No	No	2
			CVE-2024-39684	Elevation of Privilege	Moderate	No	No	1
5040427	高危	July 9, 2024—	CVE-2024-30013	Remote Code Execution	Important	No	No	2

		KB5040427 (OS Builds 19044.4651 and 19045.4651) - Microsoft Support for Windows 10 Enterprise LTSC 2021,Windows 10 IoT Enterprise LTSC 2021,Windows 10, version 22H2, all editions	CVE-2024-38079	Elevation of Privilege	Important	No	No	1
			CVE-2024-35270	Denial of Service	Important	No	No	2
			CVE-2024-38102	Denial of Service	Important	No	No	2
			CVE-2024-38062	Elevation of Privilege	Important	No	No	2
			CVE-2024-38052	Elevation of Privilege	Important	No	No	1
			CVE-2024-37972	Security Feature Bypass	Important	No	No	2
			CVE-2024-38056	Information Disclosure	Important	No	No	2
			CVE-2024-38060	Remote Code Execution	Critical	No	No	1
			CVE-2024-38066	Elevation of Privilege	Important	No	No	1
			CVE-2024-38053	Remote Code Execution	Important	No	No	2
			CVE-2024-38032	Remote Code Execution	Important	No	No	2
			CVE-2024-37989	Security Feature Bypass	Important	No	No	2
			CVE-2024-38101	Denial of Service	Important	No	No	2
			CVE-2024-38112	Spoofing	Important	No	Yes	0
			CVE-2024-38051	Remote Code Execution	Important	No	No	2
			CVE-2024-28899	Security Feature Bypass	Important	No	No	2
			CVE-2024-38091	Denial of Service	Important	No	No	2
			CVE-2024-30071	Information Disclosure	Important	No	No	2
			CVE-2024-37981	Security Feature Bypass	Important	No	No	2
			CVE-2024-38043	Elevation of Privilege	Important	No	No	2
			CVE-2024-37988	Security Feature Bypass	Important	No	No	2

			CVE-2024-38068	Denial of Service	Important	No	No	2
			CVE-2024-38064	Information Disclosure	Important	No	No	2
			CVE-2024-38022	Elevation of Privilege	Important	No	No	2
			CVE-2024-38013	Elevation of Privilege	Important	No	No	2
			CVE-2024-38065	Security Feature Bypass	Important	No	No	2
			CVE-2024-38030	Spoofing	Important	No	No	2
			CVE-2024-38047	Elevation of Privilege	Important	No	No	2
			CVE-2024-38019	Remote Code Execution	Important	No	No	2
			CVE-2024-38041	Information Disclosure	Important	No	No	2
			CVE-2024-37974	Security Feature Bypass	Important	No	No	2
			CVE-2024-38104	Remote Code Execution	Important	No	No	2
			CVE-2024-38054	Elevation of Privilege	Important	No	No	1
			CVE-2024-37984	Security Feature Bypass	Important	No	No	2
			CVE-2024-38069	Security Feature Bypass	Important	No	No	2
			CVE-2024-38010	Security Feature Bypass	Important	No	No	2
			CVE-2024-26184	Security Feature Bypass	Important	No	No	2
			CVE-2024-38055	Information Disclosure	Important	No	No	2
			CVE-2024-38034	Elevation of Privilege	Important	No	No	2
			CVE-2024-37969	Security Feature Bypass	Important	No	No	2
			CVE-2024-30098	Security Feature Bypass	Important	No	No	2
			CVE-2024-30081	Spoofing	Important	No	No	2

			CVE-2024-38033	Elevation of Privilege	Important	No	No	2
			CVE-2024-38070	Security Feature Bypass	Important	No	No	2
			CVE-2024-38105	Denial of Service	Important	No	No	2
			CVE-2024-38085	Elevation of Privilege	Important	No	No	1
			CVE-2024-38050	Elevation of Privilege	Important	No	No	2
			CVE-2024-38049	Remote Code Execution	Important	No	No	2
			CVE-2024-38048	Denial of Service	Important	No	No	2
			CVE-2024-37986	Security Feature Bypass	Important	No	No	2
			CVE-2024-38517	Elevation of Privilege	Moderate	No	No	2
			CVE-2024-37971	Security Feature Bypass	Important	No	No	2
			CVE-2024-21417	Elevation of Privilege	Important	No	No	2
			CVE-2024-38011	Security Feature Bypass	Important	No	No	2
			CVE-2024-38058	Security Feature Bypass	Important	No	No	2
			CVE-2024-37975	Security Feature Bypass	Important	No	No	2
			CVE-2024-38028	Remote Code Execution	Important	No	No	2
			CVE-2024-30079	Elevation of Privilege	Important	No	No	2
			CVE-2024-38059	Elevation of Privilege	Important	No	No	1
			CVE-2024-38017	Information Disclosure	Important	No	No	2
			CVE-2024-38027	Denial of Service	Important	No	No	2
			CVE-2024-37973	Security Feature Bypass	Important	No	No	2
			CVE-2024-3596	Spoofing	Important	No	No	2

			CVE-2024-37987	Security Feature Bypass	Important	No	No	2
			CVE-2024-38025	Remote Code Execution	Important	No	No	2
			CVE-2024-38057	Elevation of Privilege	Important	No	No	2
			CVE-2024-37970	Security Feature Bypass	Important	No	No	2
			CVE-2024-38061	Elevation of Privilege	Important	No	No	2
			CVE-2024-39684	Elevation of Privilege	Moderate	No	No	1
5040448	高危	July 9, 2024—KB5040448 (OS Build 10240.20710) - Microsoft Support for Windows 10	CVE-2024-38081	Elevation of Privilege	Important	No	No	2
			CVE-2024-38079	Elevation of Privilege	Important	No	No	1
			CVE-2024-35270	Denial of Service	Important	No	No	2
			CVE-2024-38102	Denial of Service	Important	No	No	2
			CVE-2024-38052	Elevation of Privilege	Important	No	No	1
			CVE-2024-37972	Security Feature Bypass	Important	No	No	2
			CVE-2024-38056	Information Disclosure	Important	No	No	2
			CVE-2024-38060	Remote Code Execution	Critical	No	No	1
			CVE-2024-38066	Elevation of Privilege	Important	No	No	1
			CVE-2024-38053	Remote Code Execution	Important	No	No	2
			CVE-2024-37989	Security Feature Bypass	Important	No	No	2
			CVE-2024-38101	Denial of Service	Important	No	No	2
			CVE-2024-38112	Spoofing	Important	No	Yes	0
			CVE-2024-38051	Remote Code Execution	Important	No	No	2
			CVE-2024-28899	Security Feature Bypass	Important	No	No	2

			CVE-2024-38091	Denial of Service	Important	No	No	2
			CVE-2024-30071	Information Disclosure	Important	No	No	2
			CVE-2024-37988	Security Feature Bypass	Important	No	No	2
			CVE-2024-38068	Denial of Service	Important	No	No	2
			CVE-2024-38064	Information Disclosure	Important	No	No	2
			CVE-2024-38022	Elevation of Privilege	Important	No	No	2
			CVE-2024-38013	Elevation of Privilege	Important	No	No	2
			CVE-2024-38065	Security Feature Bypass	Important	No	No	2
			CVE-2024-38030	Spoofing	Important	No	No	2
			CVE-2024-38019	Remote Code Execution	Important	No	No	2
			CVE-2024-37974	Security Feature Bypass	Important	No	No	2
			CVE-2024-38104	Remote Code Execution	Important	No	No	2
			CVE-2024-38054	Elevation of Privilege	Important	No	No	1
			CVE-2024-37984	Security Feature Bypass	Important	No	No	2
			CVE-2024-38069	Security Feature Bypass	Important	No	No	2
			CVE-2024-38010	Security Feature Bypass	Important	No	No	2
			CVE-2024-38055	Information Disclosure	Important	No	No	2
			CVE-2024-38034	Elevation of Privilege	Important	No	No	2
			CVE-2024-37969	Security Feature Bypass	Important	No	No	2
			CVE-2024-30098	Security Feature Bypass	Important	No	No	2
			CVE-2024-30081	Spoofing	Important	No	No	2

			CVE-2024-38033	Elevation of Privilege	Important	No	No	2
			CVE-2024-38105	Denial of Service	Important	No	No	2
			CVE-2024-38070	Security Feature Bypass	Important	No	No	2
			CVE-2024-38085	Elevation of Privilege	Important	No	No	1
			CVE-2024-38049	Remote Code Execution	Important	No	No	2
			CVE-2024-38050	Elevation of Privilege	Important	No	No	2
			CVE-2024-38048	Denial of Service	Important	No	No	2
			CVE-2024-37986	Security Feature Bypass	Important	No	No	2
			CVE-2024-37971	Security Feature Bypass	Important	No	No	2
			CVE-2024-38011	Security Feature Bypass	Important	No	No	2
			CVE-2024-38058	Security Feature Bypass	Important	No	No	2
			CVE-2024-37975	Security Feature Bypass	Important	No	No	2
			CVE-2024-38028	Remote Code Execution	Important	No	No	2
			CVE-2024-30079	Elevation of Privilege	Important	No	No	2
			CVE-2024-37987	Security Feature Bypass	Important	No	No	2
			CVE-2024-38017	Information Disclosure	Important	No	No	2
			CVE-2024-38027	Denial of Service	Important	No	No	2
			CVE-2024-37973	Security Feature Bypass	Important	No	No	2
			CVE-2024-3596	Spoofing	Important	No	No	2
			CVE-2024-38025	Remote Code Execution	Important	No	No	2
			CVE-2024-38057	Elevation of Privilege	Important	No	No	2

			CVE-2024-37970	Security Feature Bypass	Important	No	No	2
			CVE-2024-38061	Elevation of Privilege	Important	No	No	2
			CVE-2024-39684	Elevation of Privilege	Moderate	No	No	1
5040497	高危	July 9, 2024—KB5040497 (Monthly Rollup) - Microsoft Support for Windows Server 2008 R2 Enterprise ESU,Windows Server 2008 R2 Standard ESU,Windows Server 2008 R2 Datacenter ESU,Windows Embedded POSReady 7 ESU	CVE-2024-38079	Elevation of Privilege	Important	No	No	1
			CVE-2024-35270	Denial of Service	Important	No	No	2
			CVE-2024-38052	Elevation of Privilege	Important	No	No	1
			CVE-2024-38060	Remote Code Execution	Critical	No	No	1
			CVE-2024-38066	Elevation of Privilege	Important	No	No	1
			CVE-2024-38051	Remote Code Execution	Important	No	No	2
			CVE-2024-38091	Denial of Service	Important	No	No	2
			CVE-2024-38044	Remote Code Execution	Important	No	No	2
			CVE-2024-38071	Denial of Service	Important	No	No	2
			CVE-2024-38064	Information Disclosure	Important	No	No	2
			CVE-2024-38068	Denial of Service	Important	No	No	2
			CVE-2024-38099	Denial of Service	Important	No	No	1
			CVE-2024-38019	Remote Code Execution	Important	No	No	2
			CVE-2024-38104	Remote Code Execution	Important	No	No	2
			CVE-2024-38054	Elevation of Privilege	Important	No	No	1
			CVE-2024-38031	Denial of Service	Important	No	No	2
			CVE-2024-38055	Information Disclosure	Important	No	No	2

			CVE-2024-38034	Elevation of Privilege	Important	No	No	2
			CVE-2024-30081	Spoofing	Important	No	No	2
			CVE-2024-38085	Elevation of Privilege	Important	No	No	1
			CVE-2024-38049	Remote Code Execution	Important	No	No	2
			CVE-2024-38050	Elevation of Privilege	Important	No	No	2
			CVE-2024-38048	Denial of Service	Important	No	No	2
			CVE-2024-38077	Remote Code Execution	Critical	No	No	2
			CVE-2024-38074	Remote Code Execution	Critical	No	No	2
			CVE-2024-38073	Denial of Service	Important	No	No	2
			CVE-2024-38067	Denial of Service	Important	No	No	2
			CVE-2024-38028	Remote Code Execution	Important	No	No	2
			CVE-2024-38017	Information Disclosure	Important	No	No	2
			CVE-2024-38027	Denial of Service	Important	No	No	2
			CVE-2024-3596	Spoofing	Important	No	No	2
			CVE-2024-38025	Remote Code Execution	Important	No	No	2
			CVE-2024-38057	Elevation of Privilege	Important	No	No	2
			CVE-2024-38061	Elevation of Privilege	Important	No	No	2
			CVE-2024-39684	Elevation of Privilege	Moderate	No	No	1
5040498	高危	July 9, 2024—KB5040498 (Security-only update) -	CVE-2024-38079	Elevation of Privilege	Important	No	No	1
			CVE-2024-35270	Denial of Service	Important	No	No	2
			CVE-2024-38052	Elevation of Privilege	Important	No	No	1

		Microsoft Support for Windows Server 2008 R2 Enterprise ESU,Windows Server 2008 R2 Standard ESU,Windows Server 2008 R2 Datacenter ESU,Windows Embedded POSReady 7 ESU	CVE-2024-38060	Remote Code Execution	Critical	No	No	1
			CVE-2024-38066	Elevation of Privilege	Important	No	No	1
			CVE-2024-38051	Remote Code Execution	Important	No	No	2
			CVE-2024-38091	Denial of Service	Important	No	No	2
			CVE-2024-38044	Remote Code Execution	Important	No	No	2
			CVE-2024-38071	Denial of Service	Important	No	No	2
			CVE-2024-38064	Information Disclosure	Important	No	No	2
			CVE-2024-38068	Denial of Service	Important	No	No	2
			CVE-2024-38099	Denial of Service	Important	No	No	1
			CVE-2024-38019	Remote Code Execution	Important	No	No	2
			CVE-2024-38104	Remote Code Execution	Important	No	No	2
			CVE-2024-38054	Elevation of Privilege	Important	No	No	1
			CVE-2024-38031	Denial of Service	Important	No	No	2
			CVE-2024-38055	Information Disclosure	Important	No	No	2
			CVE-2024-38034	Elevation of Privilege	Important	No	No	2
			CVE-2024-30081	Spoofing	Important	No	No	2
			CVE-2024-38085	Elevation of Privilege	Important	No	No	1
			CVE-2024-38049	Remote Code Execution	Important	No	No	2
			CVE-2024-38050	Elevation of Privilege	Important	No	No	2
			CVE-2024-38048	Denial of Service	Important	No	No	2
			CVE-2024-38077	Remote Code Execution	Critical	No	No	2

			CVE-2024-38074	Remote Code Execution	Critical	No	No	2
			CVE-2024-38073	Denial of Service	Important	No	No	2
			CVE-2024-38067	Denial of Service	Important	No	No	2
			CVE-2024-38028	Remote Code Execution	Important	No	No	2
			CVE-2024-38017	Information Disclosure	Important	No	No	2
			CVE-2024-38027	Denial of Service	Important	No	No	2
			CVE-2024-3596	Spoofing	Important	No	No	2
			CVE-2024-38025	Remote Code Execution	Important	No	No	2
			CVE-2024-38057	Elevation of Privilege	Important	No	No	2
			CVE-2024-38061	Elevation of Privilege	Important	No	No	2
			CVE-2024-39684	Elevation of Privilege	Moderate	No	No	1
5040437	高危	July 9, 2024—KB5040437 (OS Build 20348.2582) - Microsoft Support for Windows Server 2022	CVE-2024-35270	Denial of Service	Important	No	No	2
			CVE-2024-28899	Security Feature Bypass	Important	No	No	2
			CVE-2024-38043	Elevation of Privilege	Important	No	No	2
			CVE-2024-38104	Remote Code Execution	Important	No	No	2
			CVE-2024-38031	Denial of Service	Important	No	No	2
			CVE-2024-37969	Security Feature Bypass	Important	No	No	2
			CVE-2024-38076	Remote Code Execution	Critical	No	No	2
			CVE-2024-38033	Elevation of Privilege	Important	No	No	2
			CVE-2024-38070	Security Feature Bypass	Important	No	No	2
			CVE-2024-38085	Elevation of Privilege	Important	No	No	1

			CVE-2024-38049	Remote Code Execution	Important	No	No	2
			CVE-2024-37977	Security Feature Bypass	Important	No	No	2
			CVE-2024-38077	Remote Code Execution	Critical	No	No	2
			CVE-2024-37971	Security Feature Bypass	Important	No	No	2
			CVE-2024-37974	Security Feature Bypass	Important	No	No	2
			CVE-2024-38011	Security Feature Bypass	Important	No	No	2
			CVE-2024-37987	Security Feature Bypass	Important	No	No	2
			CVE-2024-30079	Elevation of Privilege	Important	No	No	2
			CVE-2024-38027	Denial of Service	Important	No	No	2
			CVE-2024-37973	Security Feature Bypass	Important	No	No	2
			CVE-2024-38057	Elevation of Privilege	Important	No	No	2
			CVE-2024-30013	Remote Code Execution	Important	No	No	2
			CVE-2024-38052	Elevation of Privilege	Important	No	No	1
			CVE-2024-37972	Security Feature Bypass	Important	No	No	2
			CVE-2024-38053	Remote Code Execution	Important	No	No	2
			CVE-2024-38112	Spoofing	Important	No	Yes	0
			CVE-2024-30071	Information Disclosure	Important	No	No	2
			CVE-2024-37988	Security Feature Bypass	Important	No	No	2
			CVE-2024-38030	Spoofing	Important	No	No	2
			CVE-2024-38047	Elevation of Privilege	Important	No	No	2
			CVE-2024-38019	Remote Code Execution	Important	No	No	2

			CVE-2024-38055	Information Disclosure	Important	No	No	2
			CVE-2024-30081	Spoofing	Important	No	No	2
			CVE-2024-38080	Elevation of Privilege	Important	No	Yes	0
			CVE-2024-37986	Security Feature Bypass	Important	No	No	2
			CVE-2024-38517	Elevation of Privilege	Moderate	No	No	2
			CVE-2024-21417	Elevation of Privilege	Important	No	No	2
			CVE-2024-37975	Security Feature Bypass	Important	No	No	2
			CVE-2024-38073	Denial of Service	Important	No	No	2
			CVE-2024-38058	Security Feature Bypass	Important	No	No	2
			CVE-2024-38017	Information Disclosure	Important	No	No	2
			CVE-2024-3596	Spoofing	Important	No	No	2
			CVE-2024-38079	Elevation of Privilege	Important	No	No	1
			CVE-2024-38062	Elevation of Privilege	Important	No	No	2
			CVE-2024-38056	Information Disclosure	Important	No	No	2
			CVE-2024-38060	Remote Code Execution	Critical	No	No	1
			CVE-2024-37989	Security Feature Bypass	Important	No	No	2
			CVE-2024-38101	Denial of Service	Important	No	No	2
			CVE-2024-38051	Remote Code Execution	Important	No	No	2
			CVE-2024-38091	Denial of Service	Important	No	No	2
			CVE-2024-38044	Remote Code Execution	Important	No	No	2
			CVE-2024-37981	Security Feature Bypass	Important	No	No	2

			CVE-2024-38068	Denial of Service	Important	No	No	2
			CVE-2024-38022	Elevation of Privilege	Important	No	No	2
			CVE-2024-38013	Elevation of Privilege	Important	No	No	2
			CVE-2024-38065	Security Feature Bypass	Important	No	No	2
			CVE-2024-38054	Elevation of Privilege	Important	No	No	1
			CVE-2024-38069	Security Feature Bypass	Important	No	No	2
			CVE-2024-38034	Elevation of Privilege	Important	No	No	2
			CVE-2024-38105	Denial of Service	Important	No	No	2
			CVE-2024-38048	Denial of Service	Important	No	No	2
			CVE-2024-38025	Remote Code Execution	Important	No	No	2
			CVE-2024-38072	Denial of Service	Important	No	No	2
			CVE-2024-38061	Elevation of Privilege	Important	No	No	2
			CVE-2024-38102	Denial of Service	Important	No	No	2
			CVE-2024-38071	Denial of Service	Important	No	No	2
			CVE-2024-38064	Information Disclosure	Important	No	No	2
			CVE-2024-38099	Denial of Service	Important	No	No	1
			CVE-2024-38041	Information Disclosure	Important	No	No	2
			CVE-2024-38100	Elevation of Privilege	Important	No	No	1
			CVE-2024-37984	Security Feature Bypass	Important	No	No	2
			CVE-2024-30098	Security Feature Bypass	Important	No	No	2

			CVE-2024-38010	Security Feature Bypass	Important	No	No	2
			CVE-2024-26184	Security Feature Bypass	Important	No	No	2
			CVE-2024-38050	Elevation of Privilege	Important	No	No	2
			CVE-2024-38074	Remote Code Execution	Critical	No	No	2
			CVE-2024-38067	Denial of Service	Important	No	No	2
			CVE-2024-38059	Elevation of Privilege	Important	No	No	1
			CVE-2024-38028	Remote Code Execution	Important	No	No	2
			CVE-2024-38015	Denial of Service	Important	No	No	2
			CVE-2024-37970	Security Feature Bypass	Important	No	No	2
			CVE-2024-39684	Elevation of Privilege	Moderate	No	No	1
5040431	高危	July 9, 2024—KB5040431 (OS Build 22000.3079) - Microsoft Support for Windows 11 version 21H2, all editions	CVE-2024-30013	Remote Code Execution	Important	No	No	2
			CVE-2024-38079	Elevation of Privilege	Important	No	No	1
			CVE-2024-35270	Denial of Service	Important	No	No	2
			CVE-2024-38102	Denial of Service	Important	No	No	2
			CVE-2024-38062	Elevation of Privilege	Important	No	No	2
			CVE-2024-38052	Elevation of Privilege	Important	No	No	1
			CVE-2024-37972	Security Feature Bypass	Important	No	No	2
			CVE-2024-38056	Information Disclosure	Important	No	No	2
			CVE-2024-38078	Remote Code Execution	Important	No	No	2
			CVE-2024-38060	Remote Code Execution	Critical	No	No	1

			CVE-2024-38053	Remote Code Execution	Important	No	No	2
			CVE-2024-38032	Remote Code Execution	Important	No	No	2
			CVE-2024-37989	Security Feature Bypass	Important	No	No	2
			CVE-2024-38101	Denial of Service	Important	No	No	2
			CVE-2024-38112	Spoofing	Important	No	Yes	0
			CVE-2024-38051	Remote Code Execution	Important	No	No	2
			CVE-2024-28899	Security Feature Bypass	Important	No	No	2
			CVE-2024-38091	Denial of Service	Important	No	No	2
			CVE-2024-30071	Information Disclosure	Important	No	No	2
			CVE-2024-37981	Security Feature Bypass	Important	No	No	2
			CVE-2024-38043	Elevation of Privilege	Important	No	No	2
			CVE-2024-37988	Security Feature Bypass	Important	No	No	2
			CVE-2024-38068	Denial of Service	Important	No	No	2
			CVE-2024-38064	Information Disclosure	Important	No	No	2
			CVE-2024-38022	Elevation of Privilege	Important	No	No	2
			CVE-2024-38013	Elevation of Privilege	Important	No	No	2
			CVE-2024-38065	Security Feature Bypass	Important	No	No	2
			CVE-2024-38030	Spoofing	Important	No	No	2
			CVE-2024-38047	Elevation of Privilege	Important	No	No	2
			CVE-2024-38019	Remote Code Execution	Important	No	No	2
			CVE-2024-38041	Information Disclosure	Important	No	No	2

			CVE-2024-37974	Security Feature Bypass	Important	No	No	2
			CVE-2024-38104	Remote Code Execution	Important	No	No	2
			CVE-2024-38054	Elevation of Privilege	Important	No	No	1
			CVE-2024-37984	Security Feature Bypass	Important	No	No	2
			CVE-2024-38069	Security Feature Bypass	Important	No	No	2
			CVE-2024-38010	Security Feature Bypass	Important	No	No	2
			CVE-2024-26184	Security Feature Bypass	Important	No	No	2
			CVE-2024-38055	Information Disclosure	Important	No	No	2
			CVE-2024-38034	Elevation of Privilege	Important	No	No	2
			CVE-2024-37969	Security Feature Bypass	Important	No	No	2
			CVE-2024-38080	Elevation of Privilege	Important	No	Yes	0
			CVE-2024-30098	Security Feature Bypass	Important	No	No	2
			CVE-2024-38033	Elevation of Privilege	Important	No	No	2
			CVE-2024-30081	Spoofing	Important	No	No	2
			CVE-2024-38105	Denial of Service	Important	No	No	2
			CVE-2024-38070	Security Feature Bypass	Important	No	No	2
			CVE-2024-38085	Elevation of Privilege	Important	No	No	1
			CVE-2024-38050	Elevation of Privilege	Important	No	No	2
			CVE-2024-38049	Remote Code Execution	Important	No	No	2
			CVE-2024-38048	Denial of Service	Important	No	No	2
			CVE-2024-37977	Security Feature Bypass	Important	No	No	2

			CVE-2024-37986	Security Feature Bypass	Important	No	No	2
			CVE-2024-38517	Elevation of Privilege	Moderate	No	No	2
			CVE-2024-37971	Security Feature Bypass	Important	No	No	2
			CVE-2024-21417	Elevation of Privilege	Important	No	No	2
			CVE-2024-38011	Security Feature Bypass	Important	No	No	2
			CVE-2024-38058	Security Feature Bypass	Important	No	No	2
			CVE-2024-37975	Security Feature Bypass	Important	No	No	2
			CVE-2024-38028	Remote Code Execution	Important	No	No	2
			CVE-2024-30079	Elevation of Privilege	Important	No	No	2
			CVE-2024-38059	Elevation of Privilege	Important	No	No	1
			CVE-2024-38017	Information Disclosure	Important	No	No	2
			CVE-2024-38027	Denial of Service	Important	No	No	2
			CVE-2024-37973	Security Feature Bypass	Important	No	No	2
			CVE-2024-3596	Spoofing	Important	No	No	2
			CVE-2024-37987	Security Feature Bypass	Important	No	No	2
			CVE-2024-38025	Remote Code Execution	Important	No	No	2
			CVE-2024-38057	Elevation of Privilege	Important	No	No	2
			CVE-2024-37970	Security Feature Bypass	Important	No	No	2
			CVE-2024-38061	Elevation of Privilege	Important	No	No	2
			CVE-2024-39684	Elevation of Privilege	Moderate	No	No	1
5040442	高危	July 9, 2024—	CVE-2024-30013	Remote Code Execution	Important	No	No	2

		KB5040442 (OS Builds 22621.3880 and 22631.3880) - Microsoft Support for Windows 11 version 22H2, all editions, Windows 11 version 23H2, all editions	CVE-2024-38079	Elevation of Privilege	Important	No	No	1
			CVE-2024-35270	Denial of Service	Important	No	No	2
			CVE-2024-37978	Security Feature Bypass	Important	No	No	2
			CVE-2024-38102	Denial of Service	Important	No	No	2
			CVE-2024-38062	Elevation of Privilege	Important	No	No	2
			CVE-2024-38052	Elevation of Privilege	Important	No	No	1
			CVE-2024-37972	Security Feature Bypass	Important	No	No	2
			CVE-2024-38056	Information Disclosure	Important	No	No	2
			CVE-2024-38078	Remote Code Execution	Important	No	No	2
			CVE-2024-38060	Remote Code Execution	Critical	No	No	1
			CVE-2024-38053	Remote Code Execution	Important	No	No	2
			CVE-2024-38032	Remote Code Execution	Important	No	No	2
			CVE-2024-37989	Security Feature Bypass	Important	No	No	2
			CVE-2024-38101	Denial of Service	Important	No	No	2
			CVE-2024-38112	Spoofing	Important	No	Yes	0
			CVE-2024-38051	Remote Code Execution	Important	No	No	2
			CVE-2024-28899	Security Feature Bypass	Important	No	No	2
			CVE-2024-38091	Denial of Service	Important	No	No	2
			CVE-2024-30071	Information Disclosure	Important	No	No	2
			CVE-2024-37981	Security Feature Bypass	Important	No	No	2
			CVE-2024-38043	Elevation of Privilege	Important	No	No	2

			CVE-2024-37988	Security Feature Bypass	Important	No	No	2
			CVE-2024-38068	Denial of Service	Important	No	No	2
			CVE-2024-38064	Information Disclosure	Important	No	No	2
			CVE-2024-38022	Elevation of Privilege	Important	No	No	2
			CVE-2024-38013	Elevation of Privilege	Important	No	No	2
			CVE-2024-38065	Security Feature Bypass	Important	No	No	2
			CVE-2024-38030	Spoofing	Important	No	No	2
			CVE-2024-38047	Elevation of Privilege	Important	No	No	2
			CVE-2024-38019	Remote Code Execution	Important	No	No	2
			CVE-2024-38041	Information Disclosure	Important	No	No	2
			CVE-2024-37974	Security Feature Bypass	Important	No	No	2
			CVE-2024-38104	Remote Code Execution	Important	No	No	2
			CVE-2024-38054	Elevation of Privilege	Important	No	No	1
			CVE-2024-37984	Security Feature Bypass	Important	No	No	2
			CVE-2024-38069	Security Feature Bypass	Important	No	No	2
			CVE-2024-38010	Security Feature Bypass	Important	No	No	2
			CVE-2024-26184	Security Feature Bypass	Important	No	No	2
			CVE-2024-38055	Information Disclosure	Important	No	No	2
			CVE-2024-38034	Elevation of Privilege	Important	No	No	2
			CVE-2024-37969	Security Feature Bypass	Important	No	No	2
			CVE-2024-38080	Elevation of Privilege	Important	No	Yes	0

			CVE-2024-30098	Security Feature Bypass	Important	No	No	2
			CVE-2024-38033	Elevation of Privilege	Important	No	No	2
			CVE-2024-30081	Spoofing	Important	No	No	2
			CVE-2024-38070	Security Feature Bypass	Important	No	No	2
			CVE-2024-38105	Denial of Service	Important	No	No	2
			CVE-2024-38085	Elevation of Privilege	Important	No	No	1
			CVE-2024-38050	Elevation of Privilege	Important	No	No	2
			CVE-2024-38049	Remote Code Execution	Important	No	No	2
			CVE-2024-38048	Denial of Service	Important	No	No	2
			CVE-2024-37977	Security Feature Bypass	Important	No	No	2
			CVE-2024-37986	Security Feature Bypass	Important	No	No	2
			CVE-2024-38517	Elevation of Privilege	Moderate	No	No	2
			CVE-2024-37971	Security Feature Bypass	Important	No	No	2
			CVE-2024-21417	Elevation of Privilege	Important	No	No	2
			CVE-2024-37985	Information Disclosure	Important	Yes	No	2
			CVE-2024-38011	Security Feature Bypass	Important	No	No	2
			CVE-2024-38058	Security Feature Bypass	Important	No	No	2
			CVE-2024-37975	Security Feature Bypass	Important	No	No	2
			CVE-2024-38028	Remote Code Execution	Important	No	No	2
			CVE-2024-30079	Elevation of Privilege	Important	No	No	2
			CVE-2024-38059	Elevation of Privilege	Important	No	No	1

			CVE-2024-38017	Information Disclosure	Important	No	No	2
			CVE-2024-38027	Denial of Service	Important	No	No	2
			CVE-2024-37973	Security Feature Bypass	Important	No	No	2
			CVE-2024-3596	Spoofing	Important	No	No	2
			CVE-2024-37987	Security Feature Bypass	Important	No	No	2
			CVE-2024-38025	Remote Code Execution	Important	No	No	2
			CVE-2024-38057	Elevation of Privilege	Important	No	No	2
			CVE-2024-37970	Security Feature Bypass	Important	No	No	2
			CVE-2024-38061	Elevation of Privilege	Important	No	No	2
			CVE-2024-39684	Elevation of Privilege	Moderate	No	No	1

本月微软发布的软件安全更新补丁共 16 个，详细列表如下：

KBID	奇安信集团级别	补丁名称	CVE 漏洞	漏洞的影响	漏洞等级	公开披露	已受攻击	漏洞的可利用性
5041026	高危	July 9, 2024-Security Only Update for .NET Framework 3.5.1, 4.6.2, 4.7, 4.7.1,	CVE-2024-38081	Elevation of Privilege	Important	No	No	2

		4.7.2, 4.8 for Windows Server 2008 R2 SP1 (KB5041026) - Microsoft Support						
5041016	高危	July 9, 2024-KB5041016 Cumulative Update for .NET Framework 3.5, 4.8 and 4.8.1 for Windows Server 2022 - Microsoft Support	CVE-2024-38081	Elevation of Privilege	Important	No	No	2
5041017	高危	July 9, 2024-KB5041017 Cumulative Update for .NET Framework 3.5, 4.7.2 and 4.8	CVE-2024-38081	Elevation of Privilege	Important	No	No	2

		for Windows 10, version 1809 and Windows Server 2019 - Microsoft Support						
5040426	高危	KB5040426: Cumulative security update for Internet Explorer: July 9, 2024 - Microsoft Support	CVE-2024-38112	Spoofing	Important	No	Yes	0
5041027	高危	July 9, 2024-Security Only Update for .NET Framework 2.0, 3.0, 3.5 SP1, 4.6.2 for Windows Server 2008 SP2 (KB50410	CVE-2024-38081	Elevation of Privilege	Important	No	No	2

		27) - Microsoft Support						
5002621	高危	Description of the security update for Outlook 2016: July 9, 2024 (KB5002621) - Microsoft Support	CVE-2024-38020	Spoofing	Moderate	No	No	2
5039885	高危	July 9, 2024-KB5039885 Cumulative Update for .NET Framework 4.8 for Windows 10, version 1607 and Windows Server 2016 - Microsoft Support	CVE-2024-38081	Elevation of Privilege	Important	No	No	2
5041018	高危	July 9, 2024-	CVE-2024-38081	Elevation of Privilege	Important	No	No	2

		KB5041018 Cumulative Update for .NET Framework 3.5, 4.8 and 4.8.1 for Windows 10 Version 21H2 - Microsoft Support						
5041020	高危	July 9, 2024-KB5041020 Cumulative Update for .NET Framework 3.5, 4.8 and 4.8.1 for Windows 11, version 21H2 - Microsoft Support	CVE-2024-38081	Elevation of Privilege	Important	No	No	2
5041022	高危	July 9, 2024-Security and	CVE-2024-38081	Elevation of Privilege	Important	No	No	2

		Quality Rollup for .NET Framework 3.5, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Windows Server 2012 (KB5041022) - Microsoft Support						
5002618	高危	Description of the security update for SharePoint Enterprise Server 2016: July 9, 2024 (KB5002618) - Microsoft Support	CVE-2024-38024	Remote Code Execution	Important	No	No	1
			CVE-2024-38023	Remote Code Execution	Critical	No	No	1
			CVE-2024-32987	Information Disclosure	Important	No	No	2
			CVE-2024-38094	Remote Code Execution	Important	No	No	1
5041021	高危	July 9, 2024-Security and Quality	CVE-2024-38081	Elevation of Privilege	Important	No	No	2

		Rollup for .NET Framework 3.5.1, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Windows Server 2008 R2 SP1 (KB5041021) - Microsoft Support						
5041019	高危	July 9, 2024-KB5041019 Cumulative Update for .NET Framework 3.5, 4.8 and 4.8.1 for Windows 10 Version 22H2 - Microsoft Support	CVE-2024-38081	Elevation of Privilege	Important	No	No	2
5002620	高危	Description of the security	CVE-2024-38020	Spoofing	Moderate	No	No	2
			CVE-2024-38021	Remote Code Execution	Important	No	No	1

		update for Office 2016: July 9, 2024 (KB5002620) - Microsoft Support						
5041023	高危	July 9, 2024- Security and Quality Rollup for .NET Framework 3.5, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Windows Server 2012 R2 (KB5041023) - Microsoft Support	CVE-2024-38081	Elevation of Privilege	Important	No	No	2
5041024	高危	July 9, 2024- Security and Quality Rollup for .NET Framework 2.0,	CVE-2024-38081	Elevation of Privilege	Important	No	No	2

		3.0, 3.5 SP1, 4.6.2 for Windows Server 2008 SP2 (KB5041024) - Microsoft Support						

本月发布无一般性更新补丁。

注：

1、 上述表格中“漏洞的可利用性”编号详细说明如下：

0 - 已被利用(Exploitation Detected)

1 - 更有可能被利用(Exploitation More Likely)

2 - 不太可能利用(Exploitation Less Likely)

3 - 不可能利用(Exploitation Unlikely)

4 - 不受漏洞的影响(N/A)

第5章 参考链接

- Security Update Guide

https://portal.msrc.microsoft.com/zh-cn/security-guidance

- Latest non-security updates for versions of Office that use Windows Installer (MSI)

https://docs.microsoft.com/en-us/OfficeUpdates/office-msi-non-security-updates