

奇安信集团 2024 年 10 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 10 月 09 日

目 录

第 1 章 安全通告.....	2
第 2 章 重点关注补丁.....	3
第 3 章 已知问题和特殊调整.....	6
第 4 章 漏洞补丁详细列表.....	7
第 5 章 参考链接.....	52

文档信息

文档名称	奇安信集团 2024 年 10 月补丁库更新通告		
文档编号	Qi An Xin Group-MSPatch-2024-1001		
发布日期	2024-10-09	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:2024.10.09.1,V10 版本:2024.10.09.1000)已发布，本次更新推送了 31 个微软安全补丁，修复了 97 个安全漏洞，其中 10 个微软官方评级为“严重(Critical)”，87 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 13 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
5044277	CVE-2024-43582	Remote Code Execution	Critical	No	No	Exploitation Less Likely
5044284						
5044285						
5044281						
5044273						
5044280						
5044277	CVE-2024-43572	Remote Code Execution	Important	Yes	Yes	Exploitation Detected
5044284						
5044286						
5044285						
5044320						
5044343						
5044281						
5044273						
5044306						
5044321						
5044356						
5044293						
5044280						
5044342						
5044277	CVE-2024-43583	Elevation of Privilege	Important	Yes	No	Exploitation More Likely
5044284						
5044286						
5044285						
5044320						
5044343						
5044281						
5044273						

5044306						
5044321						
5044356						
5044293						
5044280						
5044342						
5044277	CVE-2024-43560	Elevation of Privilege	Important	No	No	Exploitation More Likely
5044284						
5044286						
5044285						
5044343						
5044281						
5044273						
5044293						
5044280						
5044342						
5044277	CVE-2024-6197	Remote Code Execution	Important	Yes	No	Exploitation Less Likely
5044284						
5044285						
5044281						
5044273						
5044280						
5044277	CVE-2024-43556	Elevation of Privilege	Important	No	No	Exploitation More Likely
5044284						
5044286						
5044285						
5044320						
5044343						
5044281						
5044273						
5044306						
5044321						
5044356						
5044293						
5044280						
5044342						
5044277						
5044284						
5044286						
5044285						
5044343						

5044281						
5044273						
5044293						
5044280						
5044277	CVE-2024-43509	Elevation of Privilege	Important	No	No	Exploitation More Likely
5044284						
5044286						
5044285						
5044320						
5044343						
5044281						
5044273						
5044306						
5044321						
5044356						
5044293						
5044280						
5044342						
5044277	CVE-2024-43502	Elevation of Privilege	Important	No	No	Exploitation More Likely
5044273						
5044277	CVE-2024-43615	Remote Code Execution	Important	No	No	Exploitation More Likely
5044284						
5044285						
5044281						
5044273						
5044280						
5044277	CVE-2024-43581	Remote Code Execution	Important	No	No	Exploitation More Likely
5044284						
5044285						
5044281						
5044273						
5044280						
5044277	CVE-2024-20659	Security Feature Bypass	Important	Yes	No	Exploitation Less Likely
5044284						
5044285						
5044281						
5044273						
5044280						
5002635	CVE-2024-43609	Spoofing	Important	No	No	Exploitation More 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 14 个，详细列表如下：

KBID	奇安信集团等级	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
5044277	高危	October 8, 2024—KB5044277 (OS Build 17763.6414) - Microsoft Support for Win 10 Ent LTSC 2019, Win 10 IoT Ent LTSC 2019, Windows 10 IoT Core LTSC, Windows Server 2019	CVE-2024-43582	Remote Code Execution	Critical	No	No	2
			CVE-2024-43557	Denial of Service	Important	No	No	2
			CVE-2024-43535	Elevation of Privilege	Important	No	No	2
			CVE-2024-43513	Security Feature Bypass	Important	No	No	2
			CVE-2024-43585	Security Feature Bypass	Important	No	No	2
			CVE-2024-43553	Elevation of Privilege	Important	No	No	2
			CVE-2024-43506	Denial of Service	Important	No	No	2
			CVE-2024-43567	Denial of Service	Important	No	No	2
			CVE-2024-43540	Denial of Service	Important	No	No	2
			CVE-2024-43550	Spoofing	Important	No	No	2
			CVE-2024-43456	Tampering	Important	No	No	2
			CVE-2024-43572	Remote Code Execution	Important	Yes	Yes	0
			CVE-2024-43525	Remote Code Execution	Important	No	No	2
			CVE-2024-43558	Denial of Service	Important	No	No	2

			CVE-2024-43521	Denial of Service	Important	No	No	2
			CVE-2024-43551	Elevation of Privilege	Important	No	No	2
			CVE-2024-43589	Remote Code Execution	Important	No	No	2
			CVE-2024-43524	Remote Code Execution	Important	No	No	2
			CVE-2024-43575	Denial of Service	Important	No	No	2
			CVE-2024-43583	Elevation of Privilege	Important	Yes	No	1
			CVE-2024-43518	Remote Code Execution	Important	No	No	2
			CVE-2024-43519	Remote Code Execution	Important	No	No	2
			CVE-2024-43611	Remote Code Execution	Important	No	No	2
			CVE-2024-43520	Denial of Service	Important	No	No	2
			CVE-2024-43559	Denial of Service	Important	No	No	2
			CVE-2024-43512	Denial of Service	Important	No	No	2
			CVE-2024-43555	Denial of Service	Important	No	No	2
			CVE-2024-37983	Security Feature Bypass	Important	No	No	2
			CVE-2024-43532	Elevation of Privilege	Important	No	No	2
			CVE-2024-43562	Denial of Service	Important	No	No	2
			CVE-2024-43537	Denial of Service	Important	No	No	2
			CVE-2024-43538	Denial of Service	Important	No	No	2
			CVE-2024-43565	Denial of Service	Important	No	No	2
			CVE-2024-43543	Remote Code Execution	Important	No	No	2

			CVE-2024-43560	Elevation of Privilege	Important	No	No	1
			CVE-2024-38149	Denial of Service	Important	No	No	2
			CVE-2024-43564	Remote Code Execution	Important	No	No	2
			CVE-2024-43549	Remote Code Execution	Important	No	No	2
			CVE-2024-43593	Remote Code Execution	Important	No	No	2
			CVE-2024-38124	Elevation of Privilege	Important	No	No	2
			CVE-2024-43554	Information Disclosure	Important	No	No	2
			CVE-2024-38265	Remote Code Execution	Important	No	No	2
			CVE-2024-38212	Remote Code Execution	Important	No	No	2
			CVE-2024-43608	Remote Code Execution	Important	No	No	2
			CVE-2024-38261	Remote Code Execution	Important	No	No	2
			CVE-2024-43528	Elevation of Privilege	Important	No	No	2
			CVE-2024-37982	Security Feature Bypass	Important	No	No	2
			CVE-2024-43534	Information Disclosure	Important	No	No	2
			CVE-2024-43515	Denial of Service	Important	No	No	2
			CVE-2024-43523	Remote Code Execution	Important	No	No	2
			CVE-2024-43536	Remote Code Execution	Important	No	No	2
			CVE-2024-6197	Remote Code Execution	Important	Yes	No	2
			CVE-2024-43556	Elevation of Privilege	Important	No	No	1
			CVE-2024-43573	Spoofing	Moderate	Yes	Yes	0

			CVE-2024-43511	Elevation of Privilege	Important	No	No	2
			CVE-2024-43542	Denial of Service	Important	No	No	2
			CVE-2024-43526	Remote Code Execution	Important	No	No	2
			CVE-2024-43509	Elevation of Privilege	Important	No	No	1
			CVE-2024-43607	Remote Code Execution	Important	No	No	2
			CVE-2024-43453	Remote Code Execution	Important	No	No	2
			CVE-2024-43592	Remote Code Execution	Important	No	No	2
			CVE-2024-43544	Denial of Service	Important	No	No	2
			CVE-2024-43502	Elevation of Privilege	Important	No	No	1
			CVE-2024-43517	Remote Code Execution	Important	No	No	2
			CVE-2024-37976	Security Feature Bypass	Important	No	No	2
			CVE-2024-43541	Denial of Service	Important	No	No	2
			CVE-2024-37979	Elevation of Privilege	Important	No	No	2
			CVE-2024-43514	Elevation of Privilege	Important	No	No	2
			CVE-2024-43615	Remote Code Execution	Important	No	No	1
			CVE-2024-43570	Elevation of Privilege	Important	No	No	2
			CVE-2024-43561	Denial of Service	Important	No	No	2
			CVE-2024-43599	Remote Code Execution	Important	No	No	2
			CVE-2024-43563	Elevation of Privilege	Important	No	No	2
			CVE-2024-43516	Elevation of Privilege	Important	No	No	2

			CVE-2024-43501	Elevation of Privilege	Important	No	No	2
			CVE-2024-30092	Remote Code Execution	Important	No	No	2
			CVE-2024-43581	Remote Code Execution	Important	No	No	1
			CVE-2024-43545	Denial of Service	Important	No	No	2
			CVE-2024-43547	Information Disclosure	Important	No	No	2
			CVE-2024-38262	Remote Code Execution	Important	No	No	2
			CVE-2024-20659	Security Feature Bypass	Important	Yes	No	2
5044284	高危	October 8, 2024—KB5044284 (OS Build 26100.2033) - Microsoft Support for Windows 11 version 24H2, all editions	CVE-2024-43520	Denial of Service	Important	No	No	2
			CVE-2024-43582	Remote Code Execution	Critical	No	No	2
			CVE-2024-43557	Denial of Service	Important	No	No	2
			CVE-2024-43559	Denial of Service	Important	No	No	2
			CVE-2024-43523	Remote Code Execution	Important	No	No	2
			CVE-2024-43535	Elevation of Privilege	Important	No	No	2
			CVE-2024-43513	Security Feature Bypass	Important	No	No	2
			CVE-2024-43553	Elevation of Privilege	Important	No	No	2
			CVE-2024-43585	Security Feature Bypass	Important	No	No	2
			CVE-2024-43555	Denial of Service	Important	No	No	2
			CVE-2024-43527	Elevation of Privilege	Important	No	No	2
			CVE-2024-43506	Denial of Service	Important	No	No	2

			CVE-2024-37983	Security Feature Bypass	Important	No	No	2
			CVE-2024-43536	Remote Code Execution	Important	No	No	2
			CVE-2024-6197	Remote Code Execution	Important	Yes	No	2
			CVE-2024-43540	Denial of Service	Important	No	No	2
			CVE-2024-43532	Elevation of Privilege	Important	No	No	2
			CVE-2024-43562	Denial of Service	Important	No	No	2
			CVE-2024-43571	Spoofing	Important	No	No	2
			CVE-2024-43550	Spoofing	Important	No	No	2
			CVE-2024-43537	Denial of Service	Important	No	No	2
			CVE-2024-43517	Remote Code Execution	Important	No	No	2
			CVE-2024-43572	Remote Code Execution	Important	Yes	Yes	0
			CVE-2024-37976	Security Feature Bypass	Important	No	No	2
			CVE-2024-43538	Denial of Service	Important	No	No	2
			CVE-2024-43565	Denial of Service	Important	No	No	2
			CVE-2024-43543	Remote Code Execution	Important	No	No	2
			CVE-2024-43560	Elevation of Privilege	Important	No	No	1
			CVE-2024-43558	Denial of Service	Important	No	No	2
			CVE-2024-38149	Denial of Service	Important	No	No	2
			CVE-2024-43551	Elevation of Privilege	Important	No	No	2

			CVE-2024-43500	Information Disclosure	Important	No	No	2
			CVE-2024-43525	Remote Code Execution	Important	No	No	2
			CVE-2024-43508	Information Disclosure	Important	No	No	2
			CVE-2024-43514	Elevation of Privilege	Important	No	No	2
			CVE-2024-43524	Remote Code Execution	Important	No	No	2
			CVE-2024-43615	Remote Code Execution	Important	No	No	1
			CVE-2024-43561	Denial of Service	Important	No	No	2
			CVE-2024-43570	Elevation of Privilege	Important	No	No	2
			CVE-2024-43599	Remote Code Execution	Important	No	No	2
			CVE-2024-43563	Elevation of Privilege	Important	No	No	2
			CVE-2024-43556	Elevation of Privilege	Important	No	No	1
			CVE-2024-43573	Spoofing	Moderate	Yes	Yes	0
			CVE-2024-43583	Elevation of Privilege	Important	Yes	No	1
			CVE-2024-43554	Information Disclosure	Important	No	No	2
			CVE-2024-43516	Elevation of Privilege	Important	No	No	2
			CVE-2024-43518	Remote Code Execution	Important	No	No	2
			CVE-2024-43511	Elevation of Privilege	Important	No	No	2
			CVE-2024-43542	Denial of Service	Important	No	No	2
			CVE-2024-43501	Elevation of Privilege	Important	No	No	2
			CVE-2024-30092	Remote Code Execution	Important	No	No	2
			CVE-2024-43519	Remote Code Execution	Important	No	No	2

			CVE-2024-43526	Remote Code Execution	Important	No	No	2
			CVE-2024-43581	Remote Code Execution	Important	No	No	1
			CVE-2024-43574	Remote Code Execution	Important	No	No	2
			CVE-2024-43552	Remote Code Execution	Important	No	No	2
			CVE-2024-43509	Elevation of Privilege	Important	No	No	1
			CVE-2024-43528	Elevation of Privilege	Important	No	No	2
			CVE-2024-43533	Remote Code Execution	Important	No	No	2
			CVE-2024-43547	Information Disclosure	Important	No	No	2
			CVE-2024-37982	Security Feature Bypass	Important	No	No	2
			CVE-2024-43529	Elevation of Privilege	Important	No	No	2
			CVE-2024-43546	Information Disclosure	Important	No	No	2
			CVE-2024-43534	Information Disclosure	Important	No	No	2
			CVE-2024-43515	Denial of Service	Important	No	No	2
			CVE-2024-20659	Security Feature Bypass	Important	Yes	No	2
			CVE-2024-43584	Security Feature Bypass	Important	No	No	2
5044286	高危	October 8, 2024—KB5044286 (OS Build 10240.20796) – Microsoft Support	CVE-2024-43520	Denial of Service	Important	No	No	2
			CVE-2024-43535	Elevation of Privilege	Important	No	No	2
			CVE-2024-43513	Security Feature Bypass	Important	No	No	2
			CVE-2024-43553	Elevation of Privilege	Important	No	No	2

		for Windows 10	CVE-2024-43506	Denial of Service	Important	No	No	2
			CVE-2024-37983	Security Feature Bypass	Important	No	No	2
			CVE-2024-43532	Elevation of Privilege	Important	No	No	2
			CVE-2024-43484	Denial of Service	Important	No	No	2
			CVE-2024-43562	Denial of Service	Important	No	No	2
			CVE-2024-43550	Spoofing	Important	No	No	2
			CVE-2024-43517	Remote Code Execution	Important	No	No	2
			CVE-2024-43572	Remote Code Execution	Important	Yes	Yes	0
			CVE-2024-37976	Security Feature Bypass	Important	No	No	2
			CVE-2024-43565	Denial of Service	Important	No	No	2
			CVE-2024-43560	Elevation of Privilege	Important	No	No	1
			CVE-2024-38149	Denial of Service	Important	No	No	2
			CVE-2024-43514	Elevation of Privilege	Important	No	No	2
			CVE-2024-43556	Elevation of Privilege	Important	No	No	1
			CVE-2024-43570	Elevation of Privilege	Important	No	No	2
			CVE-2024-43599	Remote Code Execution	Important	No	No	2
			CVE-2024-43563	Elevation of Privilege	Important	No	No	2
			CVE-2024-43573	Spoofing	Moderate	Yes	Yes	0
			CVE-2024-43554	Information Disclosure	Important	No	No	2
			CVE-2024-43583	Elevation of Privilege	Important	Yes	No	1

			CVE-2024-43516	Elevation of Privilege	Important	No	No	2
			CVE-2024-43518	Remote Code Execution	Important	No	No	2
			CVE-2024-43511	Elevation of Privilege	Important	No	No	2
			CVE-2024-43501	Elevation of Privilege	Important	No	No	2
			CVE-2024-30092	Remote Code Execution	Important	No	No	2
			CVE-2024-43519	Remote Code Execution	Important	No	No	2
			CVE-2024-43509	Elevation of Privilege	Important	No	No	1
			CVE-2024-43547	Information Disclosure	Important	No	No	2
			CVE-2024-37982	Security Feature Bypass	Important	No	No	2
			CVE-2024-43483	Denial of Service	Important	No	No	2
			CVE-2024-43534	Information Disclosure	Important	No	No	2
			CVE-2024-43515	Denial of Service	Important	No	No	2
5044285	高危	October 8, 2024—KB5044285 (OS Builds 22621.4317 and 22631.4317) - Microsoft Support for Windows 11 version 22H2, all editions, W	CVE-2024-43520	Denial of Service	Important	No	No	2
			CVE-2024-43582	Remote Code Execution	Critical	No	No	2
			CVE-2024-43557	Denial of Service	Important	No	No	2
			CVE-2024-43559	Denial of Service	Important	No	No	2
			CVE-2024-43523	Remote Code Execution	Important	No	No	2
			CVE-2024-43535	Elevation of Privilege	Important	No	No	2
			CVE-2024-43513	Security Feature Bypass	Important	No	No	2

	Windows 11 version 23H2, all editions	CVE-2024-43585	Security Feature Bypass	Important	No	No	2
		CVE-2024-43555	Denial of Service	Important	No	No	2
		CVE-2024-43553	Elevation of Privilege	Important	No	No	2
		CVE-2024-43522	Elevation of Privilege	Important	No	No	2
		CVE-2024-43506	Denial of Service	Important	No	No	2
		CVE-2024-37983	Security Feature Bypass	Important	No	No	2
		CVE-2024-43536	Remote Code Execution	Important	No	No	2
		CVE-2024-6197	Remote Code Execution	Important	Yes	No	2
		CVE-2024-43540	Denial of Service	Important	No	No	2
		CVE-2024-43532	Elevation of Privilege	Important	No	No	2
		CVE-2024-43562	Denial of Service	Important	No	No	2
		CVE-2024-43537	Denial of Service	Important	No	No	2
		CVE-2024-43550	Spoofing	Important	No	No	2
		CVE-2024-43517	Remote Code Execution	Important	No	No	2
		CVE-2024-43572	Remote Code Execution	Important	Yes	Yes	0
		CVE-2024-37976	Security Feature Bypass	Important	No	No	2
		CVE-2024-43538	Denial of Service	Important	No	No	2
		CVE-2024-43565	Denial of Service	Important	No	No	2
		CVE-2024-43543	Remote Code Execution	Important	No	No	2

			CVE-2024-43558	Denial of Service	Important	No	No	2
			CVE-2024-43560	Elevation of Privilege	Important	No	No	1
			CVE-2024-38149	Denial of Service	Important	No	No	2
			CVE-2024-43551	Elevation of Privilege	Important	No	No	2
			CVE-2024-43500	Information Disclosure	Important	No	No	2
			CVE-2024-43525	Remote Code Execution	Important	No	No	2
			CVE-2024-43508	Information Disclosure	Important	No	No	2
			CVE-2024-43514	Elevation of Privilege	Important	No	No	2
			CVE-2024-43524	Remote Code Execution	Important	No	No	2
			CVE-2024-43615	Remote Code Execution	Important	No	No	1
			CVE-2024-43561	Denial of Service	Important	No	No	2
			CVE-2024-43570	Elevation of Privilege	Important	No	No	2
			CVE-2024-43573	Spoofing	Moderate	Yes	Yes	0
			CVE-2024-43599	Remote Code Execution	Important	No	No	2
			CVE-2024-43563	Elevation of Privilege	Important	No	No	2
			CVE-2024-43556	Elevation of Privilege	Important	No	No	1
			CVE-2024-43583	Elevation of Privilege	Important	Yes	No	1
			CVE-2024-43554	Information Disclosure	Important	No	No	2
			CVE-2024-43516	Elevation of Privilege	Important	No	No	2
			CVE-2024-43518	Remote Code Execution	Important	No	No	2
			CVE-2024-43511	Elevation of Privilege	Important	No	No	2

			CVE-2024-43542	Denial of Service	Important	No	No	2
			CVE-2024-43501	Elevation of Privilege	Important	No	No	2
			CVE-2024-30092	Remote Code Execution	Important	No	No	2
			CVE-2024-43519	Remote Code Execution	Important	No	No	2
			CVE-2024-43526	Remote Code Execution	Important	No	No	2
			CVE-2024-43581	Remote Code Execution	Important	No	No	1
			CVE-2024-43574	Remote Code Execution	Important	No	No	2
			CVE-2024-43552	Remote Code Execution	Important	No	No	2
			CVE-2024-43509	Elevation of Privilege	Important	No	No	1
			CVE-2024-43528	Elevation of Privilege	Important	No	No	2
			CVE-2024-43533	Remote Code Execution	Important	No	No	2
			CVE-2024-43547	Information Disclosure	Important	No	No	2
			CVE-2024-37982	Security Feature Bypass	Important	No	No	2
			CVE-2024-43529	Elevation of Privilege	Important	No	No	2
			CVE-2024-43546	Information Disclosure	Important	No	No	2
			CVE-2024-43534	Information Disclosure	Important	No	No	2
			CVE-2024-43515	Denial of Service	Important	No	No	2
			CVE-2024-20659	Security Feature Bypass	Important	Yes	No	2
			CVE-2024-43584	Security Feature Bypass	Important	No	No	2

5044320	高危	October 8, 2024—	CVE-2024-43520	Denial of Service	Important	No	No	2
		KB5044320 (Monthly Rollup) – Microsoft Support for Windows Server 2008 Datacenter ESU, Windows Server 2008 Standard ESU, Windows Server 2008 Enterprise ESU	CVE-2024-43544	Denial of Service	Important	No	No	2
			CVE-2024-43535	Elevation of Privilege	Important	No	No	2
			CVE-2024-43553	Elevation of Privilege	Important	No	No	2
			CVE-2024-43532	Elevation of Privilege	Important	No	No	2
			CVE-2024-43517	Remote Code Execution	Important	No	No	2
			CVE-2024-43572	Remote Code Execution	Important	Yes	Yes	0
			CVE-2024-43541	Denial of Service	Important	No	No	2
			CVE-2024-43589	Remote Code Execution	Important	No	No	2
			CVE-2024-43564	Remote Code Execution	Important	No	No	2
			CVE-2024-43549	Remote Code Execution	Important	No	No	2
			CVE-2024-43593	Remote Code Execution	Important	No	No	2
			CVE-2024-38124	Elevation of Privilege	Important	No	No	2
			CVE-2024-43556	Elevation of Privilege	Important	No	No	1
			CVE-2024-43570	Elevation of Privilege	Important	No	No	2
			CVE-2024-43583	Elevation of Privilege	Important	Yes	No	1
			CVE-2024-43518	Remote Code Execution	Important	No	No	2
			CVE-2024-38265	Remote Code Execution	Important	No	No	2
			CVE-2024-43501	Elevation of Privilege	Important	No	No	2
			CVE-2024-43519	Remote Code Execution	Important	No	No	2

			CVE-2024-38212	Remote Code Execution	Important	No	No	2
			CVE-2024-43608	Remote Code Execution	Important	No	No	2
			CVE-2024-43509	Elevation of Privilege	Important	No	No	1
			CVE-2024-38261	Remote Code Execution	Important	No	No	2
			CVE-2024-43607	Remote Code Execution	Important	No	No	2
			CVE-2024-43545	Denial of Service	Important	No	No	2
			CVE-2024-43592	Remote Code Execution	Important	No	No	2
			CVE-2024-43453	Remote Code Execution	Important	No	No	2
			CVE-2024-43547	Information Disclosure	Important	No	No	2
			CVE-2024-38262	Remote Code Execution	Important	No	No	2
			CVE-2024-43611	Remote Code Execution	Important	No	No	2
			CVE-2024-43534	Information Disclosure	Important	No	No	2
			CVE-2024-43515	Denial of Service	Important	No	No	2
5044343	高危	October 8, 2024—KB5044343 (Monthly Rollup) – Microsoft Support for Windows Server 2012 R2 ESU	CVE-2024-43520	Denial of Service	Important	No	No	2
			CVE-2024-43544	Denial of Service	Important	No	No	2
			CVE-2024-43535	Elevation of Privilege	Important	No	No	2
			CVE-2024-43512	Denial of Service	Important	No	No	2
			CVE-2024-43513	Security Feature Bypass	Important	No	No	2
			CVE-2024-43553	Elevation of Privilege	Important	No	No	2
			CVE-2024-43506	Denial of Service	Important	No	No	2

			CVE-2024-43567	Denial of Service	Important	No	No	2
			CVE-2024-37983	Security Feature Bypass	Important	No	No	2
			CVE-2024-43532	Elevation of Privilege	Important	No	No	2
			CVE-2024-43550	Spoofing	Important	No	No	2
			CVE-2024-43517	Remote Code Execution	Important	No	No	2
			CVE-2024-43456	Tampering	Important	No	No	2
			CVE-2024-43572	Remote Code Execution	Important	Yes	Yes	0
			CVE-2024-37976	Security Feature Bypass	Important	No	No	2
			CVE-2024-43541	Denial of Service	Important	No	No	2
			CVE-2024-43560	Elevation of Privilege	Important	No	No	1
			CVE-2024-38149	Denial of Service	Important	No	No	2
			CVE-2024-43521	Denial of Service	Important	No	No	2
			CVE-2024-37979	Elevation of Privilege	Important	No	No	2
			CVE-2024-43589	Remote Code Execution	Important	No	No	2
			CVE-2024-43514	Elevation of Privilege	Important	No	No	2
			CVE-2024-43564	Remote Code Execution	Important	No	No	2
			CVE-2024-43549	Remote Code Execution	Important	No	No	2
			CVE-2024-43593	Remote Code Execution	Important	No	No	2
			CVE-2024-38124	Elevation of Privilege	Important	No	No	2

			CVE-2024-43556	Elevation of Privilege	Important	No	No	1
			CVE-2024-43570	Elevation of Privilege	Important	No	No	2
			CVE-2024-43599	Remote Code Execution	Important	No	No	2
			CVE-2024-43563	Elevation of Privilege	Important	No	No	2
			CVE-2024-43573	Spoofing	Moderate	Yes	Yes	0
			CVE-2024-43583	Elevation of Privilege	Important	Yes	No	1
			CVE-2024-43518	Remote Code Execution	Important	No	No	2
			CVE-2024-38265	Remote Code Execution	Important	No	No	2
			CVE-2024-43501	Elevation of Privilege	Important	No	No	2
			CVE-2024-43519	Remote Code Execution	Important	No	No	2
			CVE-2024-38212	Remote Code Execution	Important	No	No	2
			CVE-2024-43608	Remote Code Execution	Important	No	No	2
			CVE-2024-43509	Elevation of Privilege	Important	No	No	1
			CVE-2024-38261	Remote Code Execution	Important	No	No	2
			CVE-2024-43607	Remote Code Execution	Important	No	No	2
			CVE-2024-43545	Denial of Service	Important	No	No	2
			CVE-2024-43592	Remote Code Execution	Important	No	No	2
			CVE-2024-43453	Remote Code Execution	Important	No	No	2
			CVE-2024-43547	Information Disclosure	Important	No	No	2
			CVE-2024-38262	Remote Code Execution	Important	No	No	2

			CVE-2024-37982	Security Feature Bypass	Important	No	No	2
			CVE-2024-43611	Remote Code Execution	Important	No	No	2
			CVE-2024-43534	Information Disclosure	Important	No	No	2
			CVE-2024-43515	Denial of Service	Important	No	No	2
5044281	高危	October 8, 2024—KB5044281 (OS Build 20348.2762) - Microsoft Support for Windows Server 2022	CVE-2024-43520	Denial of Service	Important	No	No	2
			CVE-2024-43582	Remote Code Execution	Critical	No	No	2
			CVE-2024-43544	Denial of Service	Important	No	No	2
			CVE-2024-43535	Elevation of Privilege	Important	No	No	2
			CVE-2024-43512	Denial of Service	Important	No	No	2
			CVE-2024-43513	Security Feature Bypass	Important	No	No	2
			CVE-2024-43585	Security Feature Bypass	Important	No	No	2
			CVE-2024-43553	Elevation of Privilege	Important	No	No	2
			CVE-2024-43506	Denial of Service	Important	No	No	2
			CVE-2024-43567	Denial of Service	Important	No	No	2
			CVE-2024-37983	Security Feature Bypass	Important	No	No	2
			CVE-2024-6197	Remote Code Execution	Important	Yes	No	2
			CVE-2024-43532	Elevation of Privilege	Important	No	No	2
			CVE-2024-43562	Denial of Service	Important	No	No	2
CVE-2024-43550	Spoofing	Important	No	No	2			

			CVE-2024-43517	Remote Code Execution	Important	No	No	2
			CVE-2024-43456	Tampering	Important	No	No	2
			CVE-2024-43572	Remote Code Execution	Important	Yes	Yes	0
			CVE-2024-37976	Security Feature Bypass	Important	No	No	2
			CVE-2024-43565	Denial of Service	Important	No	No	2
			CVE-2024-43541	Denial of Service	Important	No	No	2
			CVE-2024-43560	Elevation of Privilege	Important	No	No	1
			CVE-2024-38149	Denial of Service	Important	No	No	2
			CVE-2024-43521	Denial of Service	Important	No	No	2
			CVE-2024-43551	Elevation of Privilege	Important	No	No	2
			CVE-2024-37979	Elevation of Privilege	Important	No	No	2
			CVE-2024-43589	Remote Code Execution	Important	No	No	2
			CVE-2024-43514	Elevation of Privilege	Important	No	No	2
			CVE-2024-43615	Remote Code Execution	Important	No	No	1
			CVE-2024-43564	Remote Code Execution	Important	No	No	2
			CVE-2024-43549	Remote Code Execution	Important	No	No	2
			CVE-2024-43593	Remote Code Execution	Important	No	No	2
			CVE-2024-38124	Elevation of Privilege	Important	No	No	2
			CVE-2024-43570	Elevation of Privilege	Important	No	No	2
			CVE-2024-43575	Denial of Service	Important	No	No	2

			CVE-2024-43573	Spoofing	Moderate	Yes	Yes	0
			CVE-2024-43599	Remote Code Execution	Important	No	No	2
			CVE-2024-43563	Elevation of Privilege	Important	No	No	2
			CVE-2024-43556	Elevation of Privilege	Important	No	No	1
			CVE-2024-43583	Elevation of Privilege	Important	Yes	No	1
			CVE-2024-43554	Information Disclosure	Important	No	No	2
			CVE-2024-43516	Elevation of Privilege	Important	No	No	2
			CVE-2024-43518	Remote Code Execution	Important	No	No	2
			CVE-2024-43511	Elevation of Privilege	Important	No	No	2
			CVE-2024-38265	Remote Code Execution	Important	No	No	2
			CVE-2024-43501	Elevation of Privilege	Important	No	No	2
			CVE-2024-30092	Remote Code Execution	Important	No	No	2
			CVE-2024-43519	Remote Code Execution	Important	No	No	2
			CVE-2024-43581	Remote Code Execution	Important	No	No	1
			CVE-2024-38212	Remote Code Execution	Important	No	No	2
			CVE-2024-43608	Remote Code Execution	Important	No	No	2
			CVE-2024-43574	Remote Code Execution	Important	No	No	2
			CVE-2024-43509	Elevation of Privilege	Important	No	No	1
			CVE-2024-38261	Remote Code Execution	Important	No	No	2
			CVE-2024-43607	Remote Code Execution	Important	No	No	2
			CVE-2024-43528	Elevation of Privilege	Important	No	No	2

			CVE-2024-43545	Denial of Service	Important	No	No	2
			CVE-2024-43592	Remote Code Execution	Important	No	No	2
			CVE-2024-43453	Remote Code Execution	Important	No	No	2
			CVE-2024-43533	Remote Code Execution	Important	No	No	2
			CVE-2024-43547	Information Disclosure	Important	No	No	2
			CVE-2024-38262	Remote Code Execution	Important	No	No	2
			CVE-2024-37982	Security Feature Bypass	Important	No	No	2
			CVE-2024-43611	Remote Code Execution	Important	No	No	2
			CVE-2024-43546	Information Disclosure	Important	No	No	2
			CVE-2024-43529	Elevation of Privilege	Important	No	No	2
			CVE-2024-43534	Information Disclosure	Important	No	No	2
			CVE-2024-43515	Denial of Service	Important	No	No	2
			CVE-2024-20659	Security Feature Bypass	Important	Yes	No	2
			CVE-2024-43584	Security Feature Bypass	Important	No	No	2
5044273	高危	October 8, 2024—KB5044273 (OS Builds 19044.5011 and 19045.5011) – Microsoft Support	CVE-2024-43520	Denial of Service	Important	No	No	2
			CVE-2024-43582	Remote Code Execution	Critical	No	No	2
			CVE-2024-43557	Denial of Service	Important	No	No	2
			CVE-2024-43559	Denial of Service	Important	No	No	2
			CVE-2024-43523	Remote Code Execution	Important	No	No	2

for Windows 10 Enterprise LTSC 2021, Windows 10 IoT Enterprise LTSC 2021, Windows 10, version 22H2, all editions	CVE-2024-43535	Elevation of Privilege	Important	No	No	2
	CVE-2024-43513	Security Feature Bypass	Important	No	No	2
	CVE-2024-43506	Denial of Service	Important	No	No	2
	CVE-2024-43585	Security Feature Bypass	Important	No	No	2
	CVE-2024-43555	Denial of Service	Important	No	No	2
	CVE-2024-43553	Elevation of Privilege	Important	No	No	2
	CVE-2024-37983	Security Feature Bypass	Important	No	No	2
	CVE-2024-43536	Remote Code Execution	Important	No	No	2
	CVE-2024-6197	Remote Code Execution	Important	Yes	No	2
	CVE-2024-43540	Denial of Service	Important	No	No	2
	CVE-2024-43532	Elevation of Privilege	Important	No	No	2
	CVE-2024-43502	Elevation of Privilege	Important	No	No	1
	CVE-2024-43562	Denial of Service	Important	No	No	2
	CVE-2024-43537	Denial of Service	Important	No	No	2
	CVE-2024-43550	Spoofing	Important	No	No	2
	CVE-2024-43517	Remote Code Execution	Important	No	No	2
	CVE-2024-43572	Remote Code Execution	Important	Yes	Yes	0
	CVE-2024-37976	Security Feature Bypass	Important	No	No	2
	CVE-2024-43538	Denial of Service	Important	No	No	2

			CVE-2024-43565	Denial of Service	Important	No	No	2
			CVE-2024-43543	Remote Code Execution	Important	No	No	2
			CVE-2024-43558	Denial of Service	Important	No	No	2
			CVE-2024-43560	Elevation of Privilege	Important	No	No	1
			CVE-2024-38149	Denial of Service	Important	No	No	2
			CVE-2024-43551	Elevation of Privilege	Important	No	No	2
			CVE-2024-43525	Remote Code Execution	Important	No	No	2
			CVE-2024-43514	Elevation of Privilege	Important	No	No	2
			CVE-2024-43524	Remote Code Execution	Important	No	No	2
			CVE-2024-43615	Remote Code Execution	Important	No	No	1
			CVE-2024-43561	Denial of Service	Important	No	No	2
			CVE-2024-43570	Elevation of Privilege	Important	No	No	2
			CVE-2024-43573	Spoofing	Moderate	Yes	Yes	0
			CVE-2024-43599	Remote Code Execution	Important	No	No	2
			CVE-2024-43563	Elevation of Privilege	Important	No	No	2
			CVE-2024-43556	Elevation of Privilege	Important	No	No	1
			CVE-2024-43583	Elevation of Privilege	Important	Yes	No	1
			CVE-2024-43554	Information Disclosure	Important	No	No	2
			CVE-2024-43516	Elevation of Privilege	Important	No	No	2
			CVE-2024-43518	Remote Code Execution	Important	No	No	2
			CVE-2024-43511	Elevation of Privilege	Important	No	No	2

			CVE-2024-43542	Denial of Service	Important	No	No	2
			CVE-2024-43501	Elevation of Privilege	Important	No	No	2
			CVE-2024-30092	Remote Code Execution	Important	No	No	2
			CVE-2024-43519	Remote Code Execution	Important	No	No	2
			CVE-2024-43526	Remote Code Execution	Important	No	No	2
			CVE-2024-43581	Remote Code Execution	Important	No	No	1
			CVE-2024-43574	Remote Code Execution	Important	No	No	2
			CVE-2024-43509	Elevation of Privilege	Important	No	No	1
			CVE-2024-43528	Elevation of Privilege	Important	No	No	2
			CVE-2024-43547	Information Disclosure	Important	No	No	2
			CVE-2024-37982	Security Feature Bypass	Important	No	No	2
			CVE-2024-43529	Elevation of Privilege	Important	No	No	2
			CVE-2024-43546	Information Disclosure	Important	No	No	2
			CVE-2024-43534	Information Disclosure	Important	No	No	2
			CVE-2024-43515	Denial of Service	Important	No	No	2
			CVE-2024-20659	Security Feature Bypass	Important	Yes	No	2
5044306	高危	October 8, 2024—KB5044306 (Security-only update) -	CVE-2024-43520	Denial of Service	Important	No	No	2
			CVE-2024-43544	Denial of Service	Important	No	No	2
			CVE-2024-43535	Elevation of Privilege	Important	No	No	2

	Microsoft Support for Windows Server 2008 Datacenter ESU, Windows Server 2008 Standard ESU, Windows Server 2008 Enterprise ESU	CVE-2024-43553	Elevation of Privilege	Important	No	No	2
		CVE-2024-43532	Elevation of Privilege	Important	No	No	2
		CVE-2024-43517	Remote Code Execution	Important	No	No	2
		CVE-2024-43572	Remote Code Execution	Important	Yes	Yes	0
		CVE-2024-43541	Denial of Service	Important	No	No	2
		CVE-2024-43589	Remote Code Execution	Important	No	No	2
		CVE-2024-43564	Remote Code Execution	Important	No	No	2
		CVE-2024-43549	Remote Code Execution	Important	No	No	2
		CVE-2024-43593	Remote Code Execution	Important	No	No	2
		CVE-2024-38124	Elevation of Privilege	Important	No	No	2
		CVE-2024-43556	Elevation of Privilege	Important	No	No	1
		CVE-2024-43570	Elevation of Privilege	Important	No	No	2
		CVE-2024-43583	Elevation of Privilege	Important	Yes	No	1
		CVE-2024-43518	Remote Code Execution	Important	No	No	2
		CVE-2024-38265	Remote Code Execution	Important	No	No	2
		CVE-2024-43501	Elevation of Privilege	Important	No	No	2
		CVE-2024-43519	Remote Code Execution	Important	No	No	2
		CVE-2024-38212	Remote Code Execution	Important	No	No	2
		CVE-2024-43608	Remote Code Execution	Important	No	No	2
		CVE-2024-43509	Elevation of Privilege	Important	No	No	1

			CVE-2024-38261	Remote Code Execution	Important	No	No	2
			CVE-2024-43607	Remote Code Execution	Important	No	No	2
			CVE-2024-43545	Denial of Service	Important	No	No	2
			CVE-2024-43592	Remote Code Execution	Important	No	No	2
			CVE-2024-43453	Remote Code Execution	Important	No	No	2
			CVE-2024-43547	Information Disclosure	Important	No	No	2
			CVE-2024-38262	Remote Code Execution	Important	No	No	2
			CVE-2024-43611	Remote Code Execution	Important	No	No	2
			CVE-2024-43534	Information Disclosure	Important	No	No	2
			CVE-2024-43515	Denial of Service	Important	No	No	2
5044321	高危	October 8, 2024—KB5044321 (Security-only update) – Microsoft Support for Windows Server 2008 R2 Enterprise ESU, Windows Server 2008 R2 Standard ESU, Windows Server 2008 R2	CVE-2024-43520	Denial of Service	Important	No	No	2
			CVE-2024-43544	Denial of Service	Important	No	No	2
			CVE-2024-43535	Elevation of Privilege	Important	No	No	2
			CVE-2024-43553	Elevation of Privilege	Important	No	No	2
			CVE-2024-43506	Denial of Service	Important	No	No	2
			CVE-2024-43532	Elevation of Privilege	Important	No	No	2
			CVE-2024-43517	Remote Code Execution	Important	No	No	2
			CVE-2024-43456	Tampering	Important	No	No	2
			CVE-2024-43572	Remote Code Execution	Important	Yes	Yes	0
			CVE-2024-43541	Denial of Service	Important	No	No	2

Datacenter ESU, Windows Embedded POSReady 7 ESU	CVE-2024-38149	Denial of Service	Important	No	No	2
	CVE-2024-43589	Remote Code Execution	Important	No	No	2
	CVE-2024-43564	Remote Code Execution	Important	No	No	2
	CVE-2024-43549	Remote Code Execution	Important	No	No	2
	CVE-2024-43593	Remote Code Execution	Important	No	No	2
	CVE-2024-38124	Elevation of Privilege	Important	No	No	2
	CVE-2024-43556	Elevation of Privilege	Important	No	No	1
	CVE-2024-43570	Elevation of Privilege	Important	No	No	2
	CVE-2024-43599	Remote Code Execution	Important	No	No	2
	CVE-2024-43583	Elevation of Privilege	Important	Yes	No	1
	CVE-2024-43518	Remote Code Execution	Important	No	No	2
	CVE-2024-38265	Remote Code Execution	Important	No	No	2
	CVE-2024-43501	Elevation of Privilege	Important	No	No	2
	CVE-2024-43519	Remote Code Execution	Important	No	No	2
	CVE-2024-38212	Remote Code Execution	Important	No	No	2
	CVE-2024-43608	Remote Code Execution	Important	No	No	2
	CVE-2024-43509	Elevation of Privilege	Important	No	No	1
	CVE-2024-38261	Remote Code Execution	Important	No	No	2
	CVE-2024-43607	Remote Code Execution	Important	No	No	2
	CVE-2024-43545	Denial of Service	Important	No	No	2

			CVE-2024-43592	Remote Code Execution	Important	No	No	2
			CVE-2024-43453	Remote Code Execution	Important	No	No	2
			CVE-2024-38262	Remote Code Execution	Important	No	No	2
			CVE-2024-43547	Information Disclosure	Important	No	No	2
			CVE-2024-43611	Remote Code Execution	Important	No	No	2
			CVE-2024-43534	Information Disclosure	Important	No	No	2
			CVE-2024-43515	Denial of Service	Important	No	No	2
5044356	高危	October 8, 2024—KB5044356 (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-2024-43520	Denial of Service	Important	No	No	2
			CVE-2024-43544	Denial of Service	Important	No	No	2
			CVE-2024-43535	Elevation of Privilege	Important	No	No	2
			CVE-2024-43553	Elevation of Privilege	Important	No	No	2
			CVE-2024-43506	Denial of Service	Important	No	No	2
			CVE-2024-43532	Elevation of Privilege	Important	No	No	2
			CVE-2024-43517	Remote Code Execution	Important	No	No	2
			CVE-2024-43456	Tampering	Important	No	No	2
			CVE-2024-43572	Remote Code Execution	Important	Yes	Yes	0
			CVE-2024-43541	Denial of Service	Important	No	No	2
			CVE-2024-38149	Denial of Service	Important	No	No	2
			CVE-2024-43589	Remote Code Execution	Important	No	No	2
			CVE-2024-43564	Remote Code Execution	Important	No	No	2

			CVE-2024-43549	Remote Code Execution	Important	No	No	2
			CVE-2024-43593	Remote Code Execution	Important	No	No	2
			CVE-2024-38124	Elevation of Privilege	Important	No	No	2
			CVE-2024-43556	Elevation of Privilege	Important	No	No	1
			CVE-2024-43570	Elevation of Privilege	Important	No	No	2
			CVE-2024-43599	Remote Code Execution	Important	No	No	2
			CVE-2024-43583	Elevation of Privilege	Important	Yes	No	1
			CVE-2024-43518	Remote Code Execution	Important	No	No	2
			CVE-2024-38265	Remote Code Execution	Important	No	No	2
			CVE-2024-43501	Elevation of Privilege	Important	No	No	2
			CVE-2024-43519	Remote Code Execution	Important	No	No	2
			CVE-2024-38212	Remote Code Execution	Important	No	No	2
			CVE-2024-43608	Remote Code Execution	Important	No	No	2
			CVE-2024-43509	Elevation of Privilege	Important	No	No	1
			CVE-2024-38261	Remote Code Execution	Important	No	No	2
			CVE-2024-43607	Remote Code Execution	Important	No	No	2
			CVE-2024-43545	Denial of Service	Important	No	No	2
			CVE-2024-43592	Remote Code Execution	Important	No	No	2
			CVE-2024-43453	Remote Code Execution	Important	No	No	2
			CVE-2024-38262	Remote Code Execution	Important	No	No	2

			CVE-2024-43547	Information Disclosure	Important	No	No	2
			CVE-2024-43611	Remote Code Execution	Important	No	No	2
			CVE-2024-43534	Information Disclosure	Important	No	No	2
			CVE-2024-43515	Denial of Service	Important	No	No	2
5044293	高危	October 8, 2024— KB5044293 (OS Build 14393.7428) — Microsoft Support for Windows 10, version 1607, all editions, Windows Server 2016, all editions	CVE-2024-43520	Denial of Service	Important	No	No	2
			CVE-2024-43544	Denial of Service	Important	No	No	2
			CVE-2024-43535	Elevation of Privilege	Important	No	No	2
			CVE-2024-43512	Denial of Service	Important	No	No	2
			CVE-2024-43513	Security Feature Bypass	Important	No	No	2
			CVE-2024-43553	Elevation of Privilege	Important	No	No	2
			CVE-2024-43506	Denial of Service	Important	No	No	2
			CVE-2024-43567	Denial of Service	Important	No	No	2
			CVE-2024-37983	Security Feature Bypass	Important	No	No	2
			CVE-2024-43532	Elevation of Privilege	Important	No	No	2
			CVE-2024-43484	Denial of Service	Important	No	No	2
			CVE-2024-43562	Denial of Service	Important	No	No	2
			CVE-2024-43550	Spoofing	Important	No	No	2
			CVE-2024-43517	Remote Code Execution	Important	No	No	2
			CVE-2024-43456	Tampering	Important	No	No	2

			CVE-2024-43572	Remote Code Execution	Important	Yes	Yes	0
			CVE-2024-37976	Security Feature Bypass	Important	No	No	2
			CVE-2024-43565	Denial of Service	Important	No	No	2
			CVE-2024-43541	Denial of Service	Important	No	No	2
			CVE-2024-43560	Elevation of Privilege	Important	No	No	1
			CVE-2024-38149	Denial of Service	Important	No	No	2
			CVE-2024-43521	Denial of Service	Important	No	No	2
			CVE-2024-43551	Elevation of Privilege	Important	No	No	2
			CVE-2024-37979	Elevation of Privilege	Important	No	No	2
			CVE-2024-43589	Remote Code Execution	Important	No	No	2
			CVE-2024-43514	Elevation of Privilege	Important	No	No	2
			CVE-2024-43564	Remote Code Execution	Important	No	No	2
			CVE-2024-43549	Remote Code Execution	Important	No	No	2
			CVE-2024-43593	Remote Code Execution	Important	No	No	2
			CVE-2024-38124	Elevation of Privilege	Important	No	No	2
			CVE-2024-43570	Elevation of Privilege	Important	No	No	2
			CVE-2024-43575	Denial of Service	Important	No	No	2
			CVE-2024-43599	Remote Code Execution	Important	No	No	2
			CVE-2024-43563	Elevation of Privilege	Important	No	No	2
			CVE-2024-43556	Elevation of Privilege	Important	No	No	1

			CVE-2024-43573	Spoofing	Moderate	Yes	Yes	0
			CVE-2024-43583	Elevation of Privilege	Important	Yes	No	1
			CVE-2024-43554	Information Disclosure	Important	No	No	2
			CVE-2024-43516	Elevation of Privilege	Important	No	No	2
			CVE-2024-43518	Remote Code Execution	Important	No	No	2
			CVE-2024-43511	Elevation of Privilege	Important	No	No	2
			CVE-2024-38265	Remote Code Execution	Important	No	No	2
			CVE-2024-43501	Elevation of Privilege	Important	No	No	2
			CVE-2024-30092	Remote Code Execution	Important	No	No	2
			CVE-2024-43519	Remote Code Execution	Important	No	No	2
			CVE-2024-38212	Remote Code Execution	Important	No	No	2
			CVE-2024-43608	Remote Code Execution	Important	No	No	2
			CVE-2024-43509	Elevation of Privilege	Important	No	No	1
			CVE-2024-38261	Remote Code Execution	Important	No	No	2
			CVE-2024-43607	Remote Code Execution	Important	No	No	2
			CVE-2024-43545	Denial of Service	Important	No	No	2
			CVE-2024-43592	Remote Code Execution	Important	No	No	2
			CVE-2024-43453	Remote Code Execution	Important	No	No	2
			CVE-2024-43547	Information Disclosure	Important	No	No	2
			CVE-2024-38262	Remote Code Execution	Important	No	No	2

			CVE-2024-37982	Security Feature Bypass	Important	No	No	2
			CVE-2024-43611	Remote Code Execution	Important	No	No	2
			CVE-2024-43483	Denial of Service	Important	No	No	2
			CVE-2024-43534	Information Disclosure	Important	No	No	2
			CVE-2024-43515	Denial of Service	Important	No	No	2
5044280	高危	October 8, 2024—KB5044280 (OS Build 22000.3260) - Microsoft Support for Windows 11 version 21H2, all editions	CVE-2024-43520	Denial of Service	Important	No	No	2
			CVE-2024-43582	Remote Code Execution	Critical	No	No	2
			CVE-2024-43557	Denial of Service	Important	No	No	2
			CVE-2024-43559	Denial of Service	Important	No	No	2
			CVE-2024-43523	Remote Code Execution	Important	No	No	2
			CVE-2024-43535	Elevation of Privilege	Important	No	No	2
			CVE-2024-43513	Security Feature Bypass	Important	No	No	2
			CVE-2024-43506	Denial of Service	Important	No	No	2
			CVE-2024-43585	Security Feature Bypass	Important	No	No	2
			CVE-2024-43555	Denial of Service	Important	No	No	2
			CVE-2024-43553	Elevation of Privilege	Important	No	No	2
			CVE-2024-37983	Security Feature Bypass	Important	No	No	2
			CVE-2024-43536	Remote Code Execution	Important	No	No	2
			CVE-2024-6197	Remote Code Execution	Important	Yes	No	2

			CVE-2024-43540	Denial of Service	Important	No	No	2
			CVE-2024-43532	Elevation of Privilege	Important	No	No	2
			CVE-2024-43562	Denial of Service	Important	No	No	2
			CVE-2024-43537	Denial of Service	Important	No	No	2
			CVE-2024-43550	Spoofing	Important	No	No	2
			CVE-2024-43517	Remote Code Execution	Important	No	No	2
			CVE-2024-43572	Remote Code Execution	Important	Yes	Yes	0
			CVE-2024-37976	Security Feature Bypass	Important	No	No	2
			CVE-2024-43538	Denial of Service	Important	No	No	2
			CVE-2024-43565	Denial of Service	Important	No	No	2
			CVE-2024-43543	Remote Code Execution	Important	No	No	2
			CVE-2024-43560	Elevation of Privilege	Important	No	No	1
			CVE-2024-43558	Denial of Service	Important	No	No	2
			CVE-2024-38149	Denial of Service	Important	No	No	2
			CVE-2024-43551	Elevation of Privilege	Important	No	No	2
			CVE-2024-43525	Remote Code Execution	Important	No	No	2
			CVE-2024-43514	Elevation of Privilege	Important	No	No	2
			CVE-2024-43524	Remote Code Execution	Important	No	No	2
			CVE-2024-43615	Remote Code Execution	Important	No	No	1
			CVE-2024-43556	Elevation of Privilege	Important	No	No	1

			CVE-2024-43561	Denial of Service	Important	No	No	2
			CVE-2024-43599	Remote Code Execution	Important	No	No	2
			CVE-2024-43563	Elevation of Privilege	Important	No	No	2
			CVE-2024-43570	Elevation of Privilege	Important	No	No	2
			CVE-2024-43573	Spoofing	Moderate	Yes	Yes	0
			CVE-2024-43583	Elevation of Privilege	Important	Yes	No	1
			CVE-2024-43554	Information Disclosure	Important	No	No	2
			CVE-2024-43516	Elevation of Privilege	Important	No	No	2
			CVE-2024-43518	Remote Code Execution	Important	No	No	2
			CVE-2024-43511	Elevation of Privilege	Important	No	No	2
			CVE-2024-43542	Denial of Service	Important	No	No	2
			CVE-2024-43501	Elevation of Privilege	Important	No	No	2
			CVE-2024-30092	Remote Code Execution	Important	No	No	2
			CVE-2024-43519	Remote Code Execution	Important	No	No	2
			CVE-2024-43526	Remote Code Execution	Important	No	No	2
			CVE-2024-43581	Remote Code Execution	Important	No	No	1
			CVE-2024-43574	Remote Code Execution	Important	No	No	2
			CVE-2024-43509	Elevation of Privilege	Important	No	No	1
			CVE-2024-43528	Elevation of Privilege	Important	No	No	2
			CVE-2024-43533	Remote Code Execution	Important	No	No	2
			CVE-2024-43547	Information Disclosure	Important	No	No	2

			CVE-2024-37982	Security Feature Bypass	Important	No	No	2
			CVE-2024-43529	Elevation of Privilege	Important	No	No	2
			CVE-2024-43546	Information Disclosure	Important	No	No	2
			CVE-2024-43534	Information Disclosure	Important	No	No	2
			CVE-2024-43515	Denial of Service	Important	No	No	2
			CVE-2024-20659	Security Feature Bypass	Important	Yes	No	2
			CVE-2024-43584	Security Feature Bypass	Important	No	No	2
5044342	高危	October 8, 2024—KB5044342 (Monthly Rollup) – Microsoft Support for Windows Server 2012 ESU	CVE-2024-43520	Denial of Service	Important	No	No	2
			CVE-2024-43544	Denial of Service	Important	No	No	2
			CVE-2024-43535	Elevation of Privilege	Important	No	No	2
			CVE-2024-43553	Elevation of Privilege	Important	No	No	2
			CVE-2024-43506	Denial of Service	Important	No	No	2
			CVE-2024-43567	Denial of Service	Important	No	No	2
			CVE-2024-37983	Security Feature Bypass	Important	No	No	2
			CVE-2024-43532	Elevation of Privilege	Important	No	No	2
			CVE-2024-43550	Spoofing	Important	No	No	2
			CVE-2024-43517	Remote Code Execution	Important	No	No	2
			CVE-2024-43456	Tampering	Important	No	No	2
			CVE-2024-43572	Remote Code Execution	Important	Yes	Yes	0

			CVE-2024-37976	Security Feature Bypass	Important	No	No	2
			CVE-2024-43541	Denial of Service	Important	No	No	2
			CVE-2024-43560	Elevation of Privilege	Important	No	No	1
			CVE-2024-38149	Denial of Service	Important	No	No	2
			CVE-2024-43521	Denial of Service	Important	No	No	2
			CVE-2024-37979	Elevation of Privilege	Important	No	No	2
			CVE-2024-43589	Remote Code Execution	Important	No	No	2
			CVE-2024-43514	Elevation of Privilege	Important	No	No	2
			CVE-2024-43564	Remote Code Execution	Important	No	No	2
			CVE-2024-43549	Remote Code Execution	Important	No	No	2
			CVE-2024-43593	Remote Code Execution	Important	No	No	2
			CVE-2024-38124	Elevation of Privilege	Important	No	No	2
			CVE-2024-43556	Elevation of Privilege	Important	No	No	1
			CVE-2024-43570	Elevation of Privilege	Important	No	No	2
			CVE-2024-43599	Remote Code Execution	Important	No	No	2
			CVE-2024-43563	Elevation of Privilege	Important	No	No	2
			CVE-2024-43583	Elevation of Privilege	Important	Yes	No	1
			CVE-2024-43518	Remote Code Execution	Important	No	No	2
			CVE-2024-38265	Remote Code Execution	Important	No	No	2
			CVE-2024-43501	Elevation of Privilege	Important	No	No	2

			CVE-2024-43519	Remote Code Execution	Important	No	No	2
			CVE-2024-38212	Remote Code Execution	Important	No	No	2
			CVE-2024-43608	Remote Code Execution	Important	No	No	2
			CVE-2024-43509	Elevation of Privilege	Important	No	No	1
			CVE-2024-38261	Remote Code Execution	Important	No	No	2
			CVE-2024-43607	Remote Code Execution	Important	No	No	2
			CVE-2024-43545	Denial of Service	Important	No	No	2
			CVE-2024-43592	Remote Code Execution	Important	No	No	2
			CVE-2024-43453	Remote Code Execution	Important	No	No	2
			CVE-2024-38262	Remote Code Execution	Important	No	No	2
			CVE-2024-43547	Information Disclosure	Important	No	No	2
			CVE-2024-37982	Security Feature Bypass	Important	No	No	2
			CVE-2024-43611	Remote Code Execution	Important	No	No	2
			CVE-2024-43534	Information Disclosure	Important	No	No	2
			CVE-2024-43515	Denial of Service	Important	No	No	2

本月微软发布的软件安全更新补丁共 17 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
5044098	高危	October 8, 2024- Security and Quality Rollup for .NET Framework 2.0, 3.0, 3.5 SP1, 4.6.2 for Windows Server 2008 SP2 (KB5044098) - Microsoft Support	CVE-2024-43483	Denial of Service	Important	No	No	2
			CVE-2024-43484	Denial of Service	Important	No	No	2
5002643	高危	Description of the security update for Excel 2016: October 8, 2024 (KB5002643) - Microsoft Support	CVE-2024-43504	Remote Code Execution	Important	No	No	2
5044085	高危	October 8, 2024- Security Only Update for .NET Framework	CVE-2024-43483	Denial of Service	Important	No	No	2
			CVE-2024-43484	Denial of Service	Important	No	No	2

		3.5.1, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Windows Server 2008 R2 SP1 (KB5044085) - Microsoft Support						
5044095	高危	October 8, 2024-	CVE-2024-43483	Denial of Service	Important	No	No	2
		Security and Quality 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 (KB5044095) - Microsoft Support	CVE-2024-43484	Denial of Service	Important	No	No	2
5044030	高危	October 8, 2024-	CVE-2024-43483	Denial of Service	Important	No	No	2
		KB5044030 Cumulative Update for .NET Framework 3.5 and 4.8.1 for Windows 11, version 24H2 - Microsoft Support	CVE-2024-43484	Denial of Service	Important	No	No	2
5044091	高危	October 8, 2024-	CVE-2024-43483	Denial of Service	Important	No	No	2

		KB5044091 Cumulative Update for .NET Framework 3.5, 4.8 and 4.8.1 for Windows 10 Version 22H2 - Microsoft Support	CVE-2024-43484	Denial of Service	Important	No	No	2
5044096	高危	October 8, 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 (KB5044096) - Microsoft Support	CVE-2024-43483	Denial of Service	Important	No	No	2
			CVE-2024-43484	Denial of Service	Important	No	No	2
5002645	高危	Description of the security update for SharePoint Enterprise Server 2016: October 8, 2024 (KB5002645) - Microsoft Support	CVE-2024-43503	Elevation of Privilege	Important	No	No	2
5044092	高危	October 8, 2024- KB5044092 Cumulative	CVE-2024-43483	Denial of Service	Important	No	No	2
			CVE-2024-43484	Denial of Service	Important	No	No	2

		Update for .NET Framework 3.5, 4.8 and 4.8.1 for Windows 11, version 21H2 - Microsoft Support						
5044089	高危	October 8, 2024- KB5044089	CVE-2024-43483	Denial of Service	Important	No	No	2
		Cumulative Update for .NET Framework 3.5, 4.7.2 and 4.8 for Windows 10, version 1809 and Windows Server 2019 - Microsoft Support	CVE-2024-43484	Denial of Service	Important	No	No	2
5044099	高危	October 8, 2024- KB5044099	CVE-2024-43483	Denial of Service	Important	No	No	2
		Cumulative Update for .NET Framework 3.5, 4.8 and 4.8.1 for Windows Server 2022 - Microsoft Support	CVE-2024-43484	Denial of Service	Important	No	No	2
5044033	高危	October 8, 2024- KB5044033	CVE-2024-43483	Denial of Service	Important	No	No	2
		Cumulative Update	CVE-2024-43484	Denial of Service	Important	No	No	2

		for .NET Framework 3.5 and 4.8.1 for Windows 11, version 22H2 and Windows 11, version 23H2 - Microsoft Support						
5044090	高危	October 8, 2024- KB5044090 Cumulative Update for .NET Framework 3.5, 4.8 and 4.8.1 for Windows 10 Version 21H2 - Microsoft Support	CVE-2024-43483	Denial of Service	Important	No	No	2
			CVE-2024-43484	Denial of Service	Important	No	No	2
5044021	高危	October 8, 2024- KB5044021 Cumulative Update for .NET Framework 4.8 for Windows 10, version 1607 and Windows Server 2016 - Microsoft Support	CVE-2024-43483	Denial of Service	Important	No	No	2
			CVE-2024-43484	Denial of Service	Important	No	No	2
5044086	高危	October 8, 2024- Security Only Update	CVE-2024-43483	Denial of Service	Important	No	No	2
			CVE-2024-43484	Denial of Service	Important	No	No	2

		for .NET Framework 2.0, 3.0, 3.5 SP1, 4.6.2 for Windows Server 2008 SP2 (KB5044086) - Microsoft Support						
5044097	高危	October 8, 2024-	CVE-2024-43483	Denial of Service	Important	No	No	2
		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 (KB5044097) - Microsoft Support	CVE-2024-43484	Denial of Service	Important	No	No	2
5002635	高危	Description of the security update for Office 2016: October 8, 2024 (KB5002635) - Microsoft Support	CVE-2024-43609	Spoofing	Important	No	No	1

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>