奇安信集团 2024 年 09 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 09 月 11 日

目 录

文档信息

文档名称	奇安信集团 2024 年 09 月补丁库更新通告		
文档编号	Qi An Xin Group-MSPatch-2024-0901		
发布日期	2024-09-11	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:2024.09.11.1,V10版本:2024.09.11.1000)已发布，本次更新推送了19个微软安全补丁，修复了55个安全漏洞，其中4个微软官方评级为“严重(Critical)”，51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 24 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
5043092	CVE-2024-43461	Spoofing	Important	No	No	Exploitation More Likely
5043076						
5043083						
5043080						
5043049						
5043087						
5043051						
5042881						
5043050						
5043067						
5043135						
5043125						
5043138						
5043064						
5043092	CVE-2024-38249	Elevation of Privilege	Important	No	No	Exploitation More Likely
5043076						
5043083						
5043129						
5043080						
5043087						
5043051						
5042881						
5043050						
5043067						
5043135						
5043125						
5043138						
5043064						

5043092	CVE-2024-38245	Elevation of Privilege	Important	No	No	Exploitation More Likely
5043076						
5043083						
5043129						
5043080						
5043087						
5043051						
5042881						
5043050						
5043067						
5043135						
5043125						
5043138						
5043064						
5043092	CVE-2024-38247	Elevation of Privilege	Important	No	No	Exploitation More Likely
5043076						
5043083						
5043129						
5043080						
5043051						
5042881						
5043050						
5043067						
5043125						
5043138						
5043064						
5043092	CVE-2024-38014	Elevation of Privilege	Important	No	Yes	Exploitation Detected
5043076						
5043083						
5043129						
5043080						
5043087						
5043051						
5042881						
5043050						
5043067						
5043135						
5043125						
5043138						
5043064						
5043092	CVE-2024-38217		Important	Yes	Yes	

5043076						
5043083						
5043129						
5043080						
5043087						
5043051		Security Feature Bypass				Exploitation Detected
5042881						
5043050						
5043067						
5043135						
5043125						
5043138						
5043064						
5043076	CVE-2024-38119	Remote Code Execution	Critical	No	No	Exploitation Less Likely
5043083						
5043080						
5043051						
5042881						
5043050						
5043067						
5043064						
5043076	CVE-2024-38253	Elevation of Privilege	Important	No	No	Exploitation More Likely
5043080						
5043067						
5043076	CVE-2024-38242	Elevation of Privilege	Important	No	No	Exploitation More Likely
5043083						
5043080						
5043051						
5042881						
5043050						
5043067						
5043064						
5043076	CVE-2024-38241	Elevation of Privilege	Important	No	No	Exploitation More Likely
5043083						
5043080						
5043051						
5042881						
5043050						
5043067						
5043064						
5043076	CVE-2024-38237		Important	No	No	

5043083						
5043080						
5043051		Elevation of Privilege				Exploitation More Likely
5042881						
5043050						
5043067						
5043064						
5043076	CVE-2024-38243	Elevation of Privilege	Important	No	No	Exploitation More Likely
5043083						
5043080						
5043051						
5042881						
5043050						
5043067						
5043064						
5043076	CVE-2024-38238	Elevation of Privilege	Important	No	No	Exploitation More Likely
5043083						
5043080						
5043051						
5042881						
5043050						
5043067						
5043064						
5043076	CVE-2024-38252	Elevation of Privilege	Important	No	No	Exploitation More Likely
5043080						
5043051						
5042881						
5043050						
5043067						
5043064						
5043076	CVE-2024-38244	Elevation of Privilege	Important	No	No	Exploitation More Likely
5043083						
5043080						
5043051						
5042881						
5043050						
5043067						
5043064						
5043076	CVE-2024-38246	Elevation of Privilege	Important	No	No	Exploitation More Likely
5043080						
5042881						

5043067 5043064						
5043083 5043051 5043050 5043125 5043138 5043064	CVE-2024-43487	Security Feature Bypass	Moderate	No	No	Exploitation More Likely
5043083	CVE-2024-43491	Remote Code Execution	Critical	No	Yes	Exploitation Detected
5043080	CVE-2024-43457	Elevation of Privilege	Important	No	No	Exploitation More Likely
5002566	CVE-2024-38226	Security Feature Bypass	Important	No	Yes	Exploitation Detected
5002624	CVE-2024-43464	Remote Code Execution	Critical	No	No	Exploitation More Likely
5002624	CVE-2024-38227	Remote Code Execution	Important	No	No	Exploitation More Likely
5002624	CVE-2024-38228	Remote Code Execution	Important	No	No	Exploitation More Likely
5002624	CVE-2024-38018	Remote Code Execution	Critical	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	奇安信等级	补丁名称	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
5043092	高危	September 10, 2024—KB5043092 (Security-only update) - 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-2024-38234	Denial of Service	Important	No	No	2
			CVE-2024-38256	Information Disclosure	Important	No	No	2
			CVE-2024-38231	Denial of Service	Important	No	No	2
			CVE-2024-43461	Spoofing	Important	No	No	1
			CVE-2024-38249	Elevation of Privilege	Important	No	No	1
			CVE-2024-38236	Denial of Service	Important	No	No	2
			CVE-2024-38263	Remote Code Execution	Important	No	No	2
			CVE-2024-38245	Elevation of Privilege	Important	No	No	1
			CVE-2024-38247	Elevation of Privilege	Important	No	No	1
			CVE-2024-38239	Elevation of Privilege	Important	No	No	2
			CVE-2024-38014	Elevation of Privilege	Important	No	Yes	0
			CVE-2024-38260	Remote Code Execution	Important	No	No	2
			CVE-2024-43467	Remote Code Execution	Important	No	No	2
			CVE-2024-38250	Elevation of Privilege	Important	No	No	2
			CVE-2024-43454	Remote Code Execution	Important	No	No	2

			CVE-2024-38217	Security Feature Bypass	Important	Yes	Yes	0
			CVE-2024-43455	Spoofing	Important	No	No	2
			CVE-2024-38138	Remote Code Execution	Important	No	No	2
			CVE-2024-30073	Security Feature Bypass	Important	No	No	2
			CVE-2024-38258	Information Disclosure	Important	No	No	2
5043076	高危	September 10, 2024—KB5043076 (OS Builds 22621.4169 and 22631.4169) - Microsoft Support for Windows 11 version 22H2, all editions,Windows 11 version 23H2, all editions	CVE-2024-38234	Denial of Service	Important	No	No	2
			CVE-2024-38119	Remote Code Execution	Critical	No	No	2
			CVE-2024-43461	Spoofing	Important	No	No	1
			CVE-2024-38257	Information Disclosure	Important	No	No	2
			CVE-2024-21416	Remote Code Execution	Important	No	No	2
			CVE-2024-38249	Elevation of Privilege	Important	No	No	1
			CVE-2024-38046	Elevation of Privilege	Important	No	No	2
			CVE-2024-38253	Elevation of Privilege	Important	No	No	1
			CVE-2024-38242	Elevation of Privilege	Important	No	No	1
			CVE-2024-38240	Elevation of Privilege	Important	No	No	2
			CVE-2024-38254	Information Disclosure	Important	No	No	2
			CVE-2024-38241	Elevation of Privilege	Important	No	No	1
			CVE-2024-38245	Elevation of Privilege	Important	No	No	1
			CVE-2024-38237	Elevation of Privilege	Important	No	No	1
			CVE-2024-38243	Elevation of Privilege	Important	No	No	1

			CVE-2024-38247	Elevation of Privilege	Important	No	No	1
			CVE-2024-38239	Elevation of Privilege	Important	No	No	2
			CVE-2024-38235	Denial of Service	Important	No	No	2
			CVE-2024-38045	Remote Code Execution	Important	No	No	2
			CVE-2024-38014	Elevation of Privilege	Important	No	Yes	0
			CVE-2024-38259	Remote Code Execution	Important	No	No	2
			CVE-2024-38238	Elevation of Privilege	Important	No	No	1
			CVE-2024-38252	Elevation of Privilege	Important	No	No	1
			CVE-2024-38244	Elevation of Privilege	Important	No	No	1
			CVE-2024-38250	Elevation of Privilege	Important	No	No	2
			CVE-2024-38248	Elevation of Privilege	Important	No	No	2
			CVE-2024-38217	Security Feature Bypass	Important	Yes	Yes	0
			CVE-2024-38246	Elevation of Privilege	Important	No	No	1
			CVE-2024-30073	Security Feature Bypass	Important	No	No	2
5043083	高危	September 10, 2024—KB5043083 (OS Build 10240.20766) - Microsoft Support for Windows 10	CVE-2024-38234	Denial of Service	Important	No	No	2
			CVE-2024-38119	Remote Code Execution	Critical	No	No	2
			CVE-2024-38256	Information Disclosure	Important	No	No	2
			CVE-2024-43461	Spoofing	Important	No	No	1
			CVE-2024-38249	Elevation of Privilege	Important	No	No	1
			CVE-2024-38046	Elevation of Privilege	Important	No	No	2

			CVE-2024-43487	Security Feature Bypass	Moderate	No	No	1
			CVE-2024-38242	Elevation of Privilege	Important	No	No	1
			CVE-2024-38254	Information Disclosure	Important	No	No	2
			CVE-2024-38240	Elevation of Privilege	Important	No	No	2
			CVE-2024-38241	Elevation of Privilege	Important	No	No	1
			CVE-2024-38245	Elevation of Privilege	Important	No	No	1
			CVE-2024-38237	Elevation of Privilege	Important	No	No	1
			CVE-2024-38243	Elevation of Privilege	Important	No	No	1
			CVE-2024-43491	Remote Code Execution	Critical	No	Yes	0
			CVE-2024-38247	Elevation of Privilege	Important	No	No	1
			CVE-2024-38239	Elevation of Privilege	Important	No	No	2
			CVE-2024-38235	Denial of Service	Important	No	No	2
			CVE-2024-38014	Elevation of Privilege	Important	No	Yes	0
			CVE-2024-38238	Elevation of Privilege	Important	No	No	1
			CVE-2024-38244	Elevation of Privilege	Important	No	No	1
			CVE-2024-38250	Elevation of Privilege	Important	No	No	2
			CVE-2024-38217	Security Feature Bypass	Important	Yes	Yes	0
			CVE-2024-30073	Security Feature Bypass	Important	No	No	2
5043129	高危	September 10, 2024—	CVE-2024-38234	Denial of Service	Important	No	No	2

		KB5043129 (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-2024-38256	Information Disclosure	Important	No	No	2
			CVE-2024-38231	Denial of Service	Important	No	No	2
			CVE-2024-38249	Elevation of Privilege	Important	No	No	1
			CVE-2024-38236	Denial of Service	Important	No	No	2
			CVE-2024-38263	Remote Code Execution	Important	No	No	2
			CVE-2024-38245	Elevation of Privilege	Important	No	No	1
			CVE-2024-38247	Elevation of Privilege	Important	No	No	1
			CVE-2024-38239	Elevation of Privilege	Important	No	No	2
			CVE-2024-38014	Elevation of Privilege	Important	No	Yes	0
			CVE-2024-38260	Remote Code Execution	Important	No	No	2
			CVE-2024-43467	Remote Code Execution	Important	No	No	2
			CVE-2024-38250	Elevation of Privilege	Important	No	No	2
			CVE-2024-43454	Remote Code Execution	Important	No	No	2
			CVE-2024-38217	Security Feature Bypass	Important	Yes	Yes	0
			CVE-2024-43455	Spoofing	Important	No	No	2
			CVE-2024-38138	Remote Code Execution	Important	No	No	2
			CVE-2024-30073	Security Feature Bypass	Important	No	No	2
			CVE-2024-38258	Information Disclosure	Important	No	No	2
5043080	高危	September 10, 2024—KB5043080 (OS Build	CVE-2024-38234	Denial of Service	Important	No	No	2
			CVE-2024-38119	Remote Code Execution	Critical	No	No	2

		26100.1742) - Microsoft Support for Windows 11 version 24H2, all editions	CVE-2024-43461	Spoofing	Important	No	No	1
			CVE-2024-21416	Remote Code Execution	Important	No	No	2
			CVE-2024-38249	Elevation of Privilege	Important	No	No	1
			CVE-2024-38046	Elevation of Privilege	Important	No	No	2
			CVE-2024-38253	Elevation of Privilege	Important	No	No	1
			CVE-2024-38242	Elevation of Privilege	Important	No	No	1
			CVE-2024-38254	Information Disclosure	Important	No	No	2
			CVE-2024-38240	Elevation of Privilege	Important	No	No	2
			CVE-2024-38241	Elevation of Privilege	Important	No	No	1
			CVE-2024-38245	Elevation of Privilege	Important	No	No	1
			CVE-2024-38237	Elevation of Privilege	Important	No	No	1
			CVE-2024-38243	Elevation of Privilege	Important	No	No	1
			CVE-2024-38247	Elevation of Privilege	Important	No	No	1
			CVE-2024-38239	Elevation of Privilege	Important	No	No	2
			CVE-2024-38235	Denial of Service	Important	No	No	2
			CVE-2024-38045	Remote Code Execution	Important	No	No	2
			CVE-2024-38014	Elevation of Privilege	Important	No	Yes	0
			CVE-2024-43457	Elevation of Privilege	Important	No	No	1
			CVE-2024-38259	Remote Code Execution	Important	No	No	2
			CVE-2024-38238	Elevation of Privilege	Important	No	No	1
			CVE-2024-38252	Elevation of Privilege	Important	No	No	1

			CVE-2024-38244	Elevation of Privilege	Important	No	No	1
			CVE-2024-38248	Elevation of Privilege	Important	No	No	2
			CVE-2024-38217	Security Feature Bypass	Important	Yes	Yes	0
			CVE-2024-38246	Elevation of Privilege	Important	No	No	1
			CVE-2024-30073	Security Feature Bypass	Important	No	No	2
5043087	高危	September 10, 2024—KB5043087 (Security-only update) - Microsoft Support for Windows Server 2008 Datacenter ESU,Windows Server 2008 Standard ESU,Windows Server 2008 Enterprise ESU	CVE-2024-38234	Denial of Service	Important	No	No	2
			CVE-2024-38256	Information Disclosure	Important	No	No	2
			CVE-2024-38231	Denial of Service	Important	No	No	2
			CVE-2024-43461	Spoofing	Important	No	No	1
			CVE-2024-43475	Information Disclosure	Important	No	No	2
			CVE-2024-38249	Elevation of Privilege	Important	No	No	1
			CVE-2024-38236	Denial of Service	Important	No	No	2
			CVE-2024-38263	Remote Code Execution	Important	No	No	2
			CVE-2024-38245	Elevation of Privilege	Important	No	No	1
			CVE-2024-38239	Elevation of Privilege	Important	No	No	2
			CVE-2024-38014	Elevation of Privilege	Important	No	Yes	0
			CVE-2024-43467	Remote Code Execution	Important	No	No	2
			CVE-2024-38250	Elevation of Privilege	Important	No	No	2
			CVE-2024-43454	Remote Code Execution	Important	No	No	2

			CVE-2024-38217	Security Feature Bypass	Important	Yes	Yes	0
			CVE-2024-43455	Spoofing	Important	No	No	2
			CVE-2024-38138	Remote Code Execution	Important	No	No	2
			CVE-2024-30073	Security Feature Bypass	Important	No	No	2
			CVE-2024-38258	Information Disclosure	Important	No	No	2
5043051	高危	September 10, 2024—KB5043051 (OS Build 14393.7336) - Microsoft Support for Windows 10, version 1607, all editions,Windows Server 2016, all editions	CVE-2024-38234	Denial of Service	Important	No	No	2
			CVE-2024-38119	Remote Code Execution	Critical	No	No	2
			CVE-2024-38256	Information Disclosure	Important	No	No	2
			CVE-2024-38231	Denial of Service	Important	No	No	2
			CVE-2024-43461	Spoofing	Important	No	No	1
			CVE-2024-38257	Information Disclosure	Important	No	No	2
			CVE-2024-38249	Elevation of Privilege	Important	No	No	1
			CVE-2024-38046	Elevation of Privilege	Important	No	No	2
			CVE-2024-43487	Security Feature Bypass	Moderate	No	No	1
			CVE-2024-38242	Elevation of Privilege	Important	No	No	1
			CVE-2024-38236	Denial of Service	Important	No	No	2
			CVE-2024-38254	Information Disclosure	Important	No	No	2
			CVE-2024-38240	Elevation of Privilege	Important	No	No	2
			CVE-2024-38263	Remote Code Execution	Important	No	No	2
			CVE-2024-38241	Elevation of Privilege	Important	No	No	1

			CVE-2024-38245	Elevation of Privilege	Important	No	No	1
			CVE-2024-38230	Denial of Service	Important	No	No	2
			CVE-2024-38237	Elevation of Privilege	Important	No	No	1
			CVE-2024-38243	Elevation of Privilege	Important	No	No	1
			CVE-2024-38247	Elevation of Privilege	Important	No	No	1
			CVE-2024-38239	Elevation of Privilege	Important	No	No	2
			CVE-2024-38235	Denial of Service	Important	No	No	2
			CVE-2024-43458	Information Disclosure	Important	No	No	2
			CVE-2024-38260	Remote Code Execution	Important	No	No	2
			CVE-2024-38232	Denial of Service	Important	No	No	2
			CVE-2024-38014	Elevation of Privilege	Important	No	Yes	0
			CVE-2024-43467	Remote Code Execution	Important	No	No	2
			CVE-2024-38238	Elevation of Privilege	Important	No	No	1
			CVE-2024-38252	Elevation of Privilege	Important	No	No	1
			CVE-2024-38244	Elevation of Privilege	Important	No	No	1
			CVE-2024-38250	Elevation of Privilege	Important	No	No	2
			CVE-2024-43454	Remote Code Execution	Important	No	No	2
			CVE-2024-38217	Security Feature Bypass	Important	Yes	Yes	0
			CVE-2024-43455	Spoofing	Important	No	No	2
			CVE-2024-30073	Security Feature Bypass	Important	No	No	2

			CVE-2024-38258	Information Disclosure	Important	No	No	2
			CVE-2024-38233	Denial of Service	Important	No	No	2
5042881	高危	September 10, 2024—KB5042881 (OS Build 20348.2700) - Microsoft Support for Windows Server 2022	CVE-2024-38234	Denial of Service	Important	No	No	2
			CVE-2024-38119	Remote Code Execution	Critical	No	No	2
			CVE-2024-38231	Denial of Service	Important	No	No	2
			CVE-2024-43461	Spoofing	Important	No	No	1
			CVE-2024-38257	Information Disclosure	Important	No	No	2
			CVE-2024-21416	Remote Code Execution	Important	No	No	2
			CVE-2024-38249	Elevation of Privilege	Important	No	No	1
			CVE-2024-38046	Elevation of Privilege	Important	No	No	2
			CVE-2024-38242	Elevation of Privilege	Important	No	No	1
			CVE-2024-38236	Denial of Service	Important	No	No	2
			CVE-2024-38254	Information Disclosure	Important	No	No	2
			CVE-2024-38240	Elevation of Privilege	Important	No	No	2
			CVE-2024-38263	Remote Code Execution	Important	No	No	2
			CVE-2024-38241	Elevation of Privilege	Important	No	No	1
			CVE-2024-38245	Elevation of Privilege	Important	No	No	1
			CVE-2024-38230	Denial of Service	Important	No	No	2
			CVE-2024-38237	Elevation of Privilege	Important	No	No	1
			CVE-2024-38243	Elevation of Privilege	Important	No	No	1
			CVE-2024-38247	Elevation of Privilege	Important	No	No	1

			CVE-2024-38239	Elevation of Privilege	Important	No	No	2
			CVE-2024-38235	Denial of Service	Important	No	No	2
			CVE-2024-38045	Remote Code Execution	Important	No	No	2
			CVE-2024-38260	Remote Code Execution	Important	No	No	2
			CVE-2024-38014	Elevation of Privilege	Important	No	Yes	0
			CVE-2024-43467	Remote Code Execution	Important	No	No	2
			CVE-2024-38259	Remote Code Execution	Important	No	No	2
			CVE-2024-38238	Elevation of Privilege	Important	No	No	1
			CVE-2024-38252	Elevation of Privilege	Important	No	No	1
			CVE-2024-38244	Elevation of Privilege	Important	No	No	1
			CVE-2024-38250	Elevation of Privilege	Important	No	No	2
			CVE-2024-43454	Remote Code Execution	Important	No	No	2
			CVE-2024-38248	Elevation of Privilege	Important	No	No	2
			CVE-2024-38217	Security Feature Bypass	Important	Yes	Yes	0
			CVE-2024-43455	Spoofing	Important	No	No	2
			CVE-2024-38246	Elevation of Privilege	Important	No	No	1
			CVE-2024-30073	Security Feature Bypass	Important	No	No	2
			CVE-2024-38258	Information Disclosure	Important	No	No	2
5043050	高危	September 10, 2024—KB5043050 (OS Build	CVE-2024-38234	Denial of Service	Important	No	No	2
			CVE-2024-38119	Remote Code Execution	Critical	No	No	2

		17763.6293) - Microsoft Support for Win 10 Ent LTSC 2019,Win 10 IoT Ent LTSC 2019,Windows 10 IoT Core LTSC,Windows Server 2019	CVE-2024-38256	Information Disclosure	Important	No	No	2
			CVE-2024-38231	Denial of Service	Important	No	No	2
			CVE-2024-43461	Spoofing	Important	No	No	1
			CVE-2024-38257	Information Disclosure	Important	No	No	2
			CVE-2024-21416	Remote Code Execution	Important	No	No	2
			CVE-2024-38249	Elevation of Privilege	Important	No	No	1
			CVE-2024-38046	Elevation of Privilege	Important	No	No	2
			CVE-2024-43487	Security Feature Bypass	Moderate	No	No	1
			CVE-2024-38242	Elevation of Privilege	Important	No	No	1
			CVE-2024-38236	Denial of Service	Important	No	No	2
			CVE-2024-38254	Information Disclosure	Important	No	No	2
			CVE-2024-38240	Elevation of Privilege	Important	No	No	2
			CVE-2024-38263	Remote Code Execution	Important	No	No	2
			CVE-2024-38241	Elevation of Privilege	Important	No	No	1
			CVE-2024-38245	Elevation of Privilege	Important	No	No	1
			CVE-2024-38230	Denial of Service	Important	No	No	2
			CVE-2024-38237	Elevation of Privilege	Important	No	No	1
			CVE-2024-38243	Elevation of Privilege	Important	No	No	1
			CVE-2024-38247	Elevation of Privilege	Important	No	No	1
			CVE-2024-38239	Elevation of Privilege	Important	No	No	2

			CVE-2024-38235	Denial of Service	Important	No	No	2
			CVE-2024-38014	Elevation of Privilege	Important	No	Yes	0
			CVE-2024-38045	Remote Code Execution	Important	No	No	2
			CVE-2024-38260	Remote Code Execution	Important	No	No	2
			CVE-2024-43467	Remote Code Execution	Important	No	No	2
			CVE-2024-38238	Elevation of Privilege	Important	No	No	1
			CVE-2024-38252	Elevation of Privilege	Important	No	No	1
			CVE-2024-38244	Elevation of Privilege	Important	No	No	1
			CVE-2024-38250	Elevation of Privilege	Important	No	No	2
			CVE-2024-43454	Remote Code Execution	Important	No	No	2
			CVE-2024-38217	Security Feature Bypass	Important	Yes	Yes	0
			CVE-2024-43455	Spoofing	Important	No	No	2
			CVE-2024-30073	Security Feature Bypass	Important	No	No	2
			CVE-2024-38258	Information Disclosure	Important	No	No	2
5043067	高危	September 10, 2024—KB5043067 (OS Build 22000.3197) - Microsoft Support for Windows 11 version	CVE-2024-38234	Denial of Service	Important	No	No	2
			CVE-2024-38119	Remote Code Execution	Critical	No	No	2
			CVE-2024-43461	Spoofing	Important	No	No	1
			CVE-2024-38257	Information Disclosure	Important	No	No	2
			CVE-2024-21416	Remote Code Execution	Important	No	No	2
			CVE-2024-38249	Elevation of Privilege	Important	No	No	1

		21H2, all editions	CVE-2024-38046	Elevation of Privilege	Important	No	No	2
			CVE-2024-38253	Elevation of Privilege	Important	No	No	1
			CVE-2024-38242	Elevation of Privilege	Important	No	No	1
			CVE-2024-38254	Information Disclosure	Important	No	No	2
			CVE-2024-38240	Elevation of Privilege	Important	No	No	2
			CVE-2024-38241	Elevation of Privilege	Important	No	No	1
			CVE-2024-38245	Elevation of Privilege	Important	No	No	1
			CVE-2024-38237	Elevation of Privilege	Important	No	No	1
			CVE-2024-38243	Elevation of Privilege	Important	No	No	1
			CVE-2024-38247	Elevation of Privilege	Important	No	No	1
			CVE-2024-38239	Elevation of Privilege	Important	No	No	2
			CVE-2024-38235	Denial of Service	Important	No	No	2
			CVE-2024-38045	Remote Code Execution	Important	No	No	2
			CVE-2024-38014	Elevation of Privilege	Important	No	Yes	0
			CVE-2024-38259	Remote Code Execution	Important	No	No	2
			CVE-2024-38238	Elevation of Privilege	Important	No	No	1
			CVE-2024-38252	Elevation of Privilege	Important	No	No	1
			CVE-2024-38244	Elevation of Privilege	Important	No	No	1
			CVE-2024-38250	Elevation of Privilege	Important	No	No	2
			CVE-2024-38248	Elevation of Privilege	Important	No	No	2

			CVE-2024-38217	Security Feature Bypass	Important	Yes	Yes	0
			CVE-2024-38246	Elevation of Privilege	Important	No	No	1
			CVE-2024-30073	Security Feature Bypass	Important	No	No	2
5043135	高危	September 10, 2024—KB5043135 (Monthly Rollup) - Microsoft Support for Windows Server 2008 Datacenter ESU,Windows Server 2008 Standard ESU,Windows Server 2008 Enterprise ESU	CVE-2024-38234	Denial of Service	Important	No	No	2
			CVE-2024-38256	Information Disclosure	Important	No	No	2
			CVE-2024-38231	Denial of Service	Important	No	No	2
			CVE-2024-43461	Spoofing	Important	No	No	1
			CVE-2024-43475	Information Disclosure	Important	No	No	2
			CVE-2024-38249	Elevation of Privilege	Important	No	No	1
			CVE-2024-38236	Denial of Service	Important	No	No	2
			CVE-2024-38263	Remote Code Execution	Important	No	No	2
			CVE-2024-38245	Elevation of Privilege	Important	No	No	1
			CVE-2024-38239	Elevation of Privilege	Important	No	No	2
			CVE-2024-38014	Elevation of Privilege	Important	No	Yes	0
			CVE-2024-43467	Remote Code Execution	Important	No	No	2
			CVE-2024-38250	Elevation of Privilege	Important	No	No	2
			CVE-2024-43454	Remote Code Execution	Important	No	No	2
			CVE-2024-38217	Security Feature Bypass	Important	Yes	Yes	0
			CVE-2024-43455	Spoofing	Important	No	No	2
			CVE-2024-38138	Remote Code Execution	Important	No	No	2

			CVE-2024-30073	Security Feature Bypass	Important	No	No	2
			CVE-2024-38258	Information Disclosure	Important	No	No	2
5043125	高危	September 10, 2024—KB5043125 (Monthly Rollup) - Microsoft Support for Windows Server 2012 ESU	CVE-2024-38234	Denial of Service	Important	No	No	2
			CVE-2024-38256	Information Disclosure	Important	No	No	2
			CVE-2024-38231	Denial of Service	Important	No	No	2
			CVE-2024-43461	Spoofing	Important	No	No	1
			CVE-2024-38249	Elevation of Privilege	Important	No	No	1
			CVE-2024-43487	Security Feature Bypass	Moderate	No	No	1
			CVE-2024-38236	Denial of Service	Important	No	No	2
			CVE-2024-38263	Remote Code Execution	Important	No	No	2
			CVE-2024-38245	Elevation of Privilege	Important	No	No	1
			CVE-2024-38247	Elevation of Privilege	Important	No	No	1
			CVE-2024-38239	Elevation of Privilege	Important	No	No	2
			CVE-2024-38014	Elevation of Privilege	Important	No	Yes	0
			CVE-2024-38260	Remote Code Execution	Important	No	No	2
			CVE-2024-43467	Remote Code Execution	Important	No	No	2
			CVE-2024-38250	Elevation of Privilege	Important	No	No	2
			CVE-2024-43454	Remote Code Execution	Important	No	No	2
			CVE-2024-38217	Security Feature Bypass	Important	Yes	Yes	0
			CVE-2024-43455	Spoofing	Important	No	No	2

			CVE-2024-38138	Remote Code Execution	Important	No	No	2
			CVE-2024-30073	Security Feature Bypass	Important	No	No	2
			CVE-2024-38258	Information Disclosure	Important	No	No	2
5043138	高危	September 10, 2024—KB5043138 (Monthly Rollup) - Microsoft Support for Windows Server 2012 R2 ESU	CVE-2024-38234	Denial of Service	Important	No	No	2
			CVE-2024-38256	Information Disclosure	Important	No	No	2
			CVE-2024-38231	Denial of Service	Important	No	No	2
			CVE-2024-43461	Spoofing	Important	No	No	1
			CVE-2024-38249	Elevation of Privilege	Important	No	No	1
			CVE-2024-43487	Security Feature Bypass	Moderate	No	No	1
			CVE-2024-38236	Denial of Service	Important	No	No	2
			CVE-2024-38240	Elevation of Privilege	Important	No	No	2
			CVE-2024-38263	Remote Code Execution	Important	No	No	2
			CVE-2024-38245	Elevation of Privilege	Important	No	No	1
			CVE-2024-38230	Denial of Service	Important	No	No	2
			CVE-2024-38247	Elevation of Privilege	Important	No	No	1
			CVE-2024-38239	Elevation of Privilege	Important	No	No	2
			CVE-2024-38014	Elevation of Privilege	Important	No	Yes	0
			CVE-2024-38260	Remote Code Execution	Important	No	No	2
			CVE-2024-43467	Remote Code Execution	Important	No	No	2
			CVE-2024-38250	Elevation of Privilege	Important	No	No	2

			CVE-2024-43454	Remote Code Execution	Important	No	No	2
			CVE-2024-38217	Security Feature Bypass	Important	Yes	Yes	0
			CVE-2024-43455	Spoofing	Important	No	No	2
			CVE-2024-38138	Remote Code Execution	Important	No	No	2
			CVE-2024-30073	Security Feature Bypass	Important	No	No	2
			CVE-2024-38258	Information Disclosure	Important	No	No	2
5043064	高危	September 10, 2024—KB5043064 (OS Builds 19044.4894 and 19045.4894) - Microsoft Support for Windows 10 Enterprise LTSC 2021,Windows 10 IoT Enterprise LTSC 2021,Windows 10, version 22H2, all editions	CVE-2024-38234	Denial of Service	Important	No	No	2
			CVE-2024-38119	Remote Code Execution	Critical	No	No	2
			CVE-2024-38256	Information Disclosure	Important	No	No	2
			CVE-2024-43461	Spoofing	Important	No	No	1
			CVE-2024-38257	Information Disclosure	Important	No	No	2
			CVE-2024-21416	Remote Code Execution	Important	No	No	2
			CVE-2024-38249	Elevation of Privilege	Important	No	No	1
			CVE-2024-38046	Elevation of Privilege	Important	No	No	2
			CVE-2024-43487	Security Feature Bypass	Moderate	No	No	1
			CVE-2024-38242	Elevation of Privilege	Important	No	No	1
			CVE-2024-38240	Elevation of Privilege	Important	No	No	2
			CVE-2024-38254	Information Disclosure	Important	No	No	2
			CVE-2024-38241	Elevation of Privilege	Important	No	No	1
			CVE-2024-38245	Elevation of Privilege	Important	No	No	1

			CVE-2024-38237	Elevation of Privilege	Important	No	No	1
			CVE-2024-38243	Elevation of Privilege	Important	No	No	1
			CVE-2024-38247	Elevation of Privilege	Important	No	No	1
			CVE-2024-38239	Elevation of Privilege	Important	No	No	2
			CVE-2024-38235	Denial of Service	Important	No	No	2
			CVE-2024-38045	Remote Code Execution	Important	No	No	2
			CVE-2024-38014	Elevation of Privilege	Important	No	Yes	0
			CVE-2024-38238	Elevation of Privilege	Important	No	No	1
			CVE-2024-38252	Elevation of Privilege	Important	No	No	1
			CVE-2024-38244	Elevation of Privilege	Important	No	No	1
			CVE-2024-38250	Elevation of Privilege	Important	No	No	2
			CVE-2024-38248	Elevation of Privilege	Important	No	No	2
			CVE-2024-38217	Security Feature Bypass	Important	Yes	Yes	0
			CVE-2024-38246	Elevation of Privilege	Important	No	No	1
			CVE-2024-30073	Security Feature Bypass	Important	No	No	2

本月微软发布的软件安全更新补丁共 5 个，详细列表如下：

KBID	奇安信等级	补丁名称	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
5002566	高危	Description of the security update for Publisher 2016: September 10, 2024 (KB5002566) - Microsoft Support	CVE-2024-38226	Security Feature Bypass	Important	No	Yes	0
5043049	高危	KB5043049: Cumulative security update for Internet Explorer: September 10, 2024 - Microsoft Support	CVE-2024-30073	Security Feature Bypass	Important	No	No	2
			CVE-2024-43461	Spoofing	Important	No	No	1
5002624	高危	Description of the security update for SharePoint Enterprise Server 2016: September 10, 2024 (KB5002624) -	CVE-2024-43466	Denial of Service	Important	No	No	2
			CVE-2024-43464	Remote Code Execution	Critical	No	No	1
			CVE-2024-38227	Remote Code Execution	Important	No	No	1
			CVE-2024-38228	Remote Code Execution	Important	No	No	1

		Microsoft Support	CVE-2024-38018	Remote Code Execution	Critical	No	No	1
5002605	高危	Description of the security update for Excel 2016: September 10, 2024 (KB5002605) - Microsoft Support	CVE-2024-43465	Elevation of Privilege	Important	No	No	2
5002634	高危	Description of the security update for Visio 2016: September 10, 2024 (KB5002634) - Microsoft Support	CVE-2024-43463	Remote Code Execution	Important	No	No	2

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