

奇安信集团 2024 年 12 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 12 月 11 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.....	8
第 4 章 漏洞补丁详细列表.....	9
第 5 章 参考链接.....	35

文档信息

文档名称	奇安信集团 2024 年 12 月补丁库更新通告		
文档编号	Qi An Xin Group-MSPatch-2024-1201		
发布日期	2024-12-11	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:2024.12.11.1,V10 版本:2024.12.11.1000)已发布，本次更新推送了 21 个微软安全补丁，修复了 69 个安全漏洞，其中 17 个微软官方评级为“严重(Critical)”，52 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 23 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	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
5048695	CVE-2024-49118	Remote Code Execution	Critical	No	No	Exploitation Less Likely
5048710						
5048652						
5048735						
5048667						
5048699						
5048671						
5048661						
5048744						
5048676						
5048685						
5048654						
5048703						
5048695	CVE-2024-49105	Remote Code Execution	Critical	No	No	Exploitation Less Likely
5048652						
5048735						
5048667						
5048699						
5048671						
5048661						
5048676						
5048685						
5048654						
5048703						
5048695	CVE-2024-49090	Elevation of Privilege	Important	No	No	Exploitation More Likely
5048710						
5048652						
5048735						

5048667						
5048699						
5048671						
5048661						
5048744						
5048676						
5048685						
5048654						
5048703						
5048695	CVE-2024-49126	Remote Code Execution	Critical	No	No	Exploitation Less Likely
5048710						
5048652						
5048735						
5048667						
5048699						
5048671						
5048661						
5048744						
5048676						
5048685	CVE-2024-49112	Remote Code Execution	Critical	No	No	Exploitation Less Likely
5048654						
5048703						
5048695						
5048710						
5048652						
5048735						
5048667						
5048699						
5048671						
5048661	CVE-2024-49127	Remote Code Execution	Critical	No	No	Exploitation Less Likely
5048744						
5048676						
5048685						
5048654						
5048703						

5048671						
5048661						
5048744						
5048676						
5048685						
5048654						
5048703						
5048695	CVE-2024-49124	Remote Code Execution	Critical	No	No	Exploitation Less Likely
5048710						
5048652						
5048735						
5048667						
5048699						
5048671						
5048661						
5048744						
5048676						
5048685						
5048654						
5048703						
5048695	CVE-2024-49122	Remote Code Execution	Critical	No	No	Exploitation More Likely
5048710						
5048652						
5048735						
5048667						
5048699						
5048671						
5048661						
5048744						
5048676						
5048685						
5048654						
5048703						
5048695	CVE-2024-49138	Elevation of Privilege	Important	Yes	Yes	Exploitation Detected
5048710						
5048652						
5048735						
5048667						
5048699						
5048671						
5048661						

5048744						
5048676						
5048685						
5048654						
5048703						
5048695	CVE-2024-49088	Elevation of Privilege	Important	No	No	Exploitation More Likely
5048710						
5048652						
5048735						
5048667						
5048699						
5048671						
5048661						
5048744						
5048676						
5048685						
5048654						
5048703						
5048652	CVE-2024-49132	Remote Code Execution	Critical	No	No	Exploitation Less Likely
5048667						
5048661						
5048685						
5048654						
5048652	CVE-2024-49123	Remote Code Execution	Critical	No	No	Exploitation Less Likely
5048667						
5048661						
5048685						
5048654						
5048652	CVE-2024-49114	Elevation of Privilege	Important	No	No	Exploitation More Likely
5048667						
5048661						
5048685						
5048654						
5048735	CVE-2024-49128	Remote Code Execution	Critical	No	No	Exploitation Less Likely
5048667						
5048699						
5048671						
5048661						
5048654						
5048735	CVE-2024-49120	Remote Code Execution	Critical	No	No	Exploitation Less Likely
5048667						

5048699						
5048671						
5048661						
5048654						
5048667	CVE-2024-49108	Remote Code Execution	Critical	No	No	Exploitation Less Likely
5048671						
5048661						
5048654						
5048667	CVE-2024-49116	Remote Code Execution	Critical	No	No	Exploitation Less Likely
5048671						
5048661						
5048654						
5048667	CVE-2024-49115	Remote Code Execution	Critical	No	No	Exploitation Less Likely
5048671						
5048661						
5048654						
5048667	CVE-2024-49117	Remote Code Execution	Critical	No	No	Exploitation Less Likely
5048685						
5048654						
5048667	CVE-2024-49093	Elevation of Privilege	Important	No	No	Exploitation More Likely
5048667	CVE-2024-49106	Remote Code Execution	Critical	No	No	Exploitation Less Likely
5048671						
5048661						
5048654						
5048667	CVE-2024-49119	Remote Code Execution	Critical	No	No	Exploitation Less Likely
5048671						
5048661						
5048654						
5002544	CVE-2024-49070	Remote Code Execution	Important	No	No	Exploitation More Likely
5002659						

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
5048695	高危	December 10, 2024—KB5048695 (Monthly Rollup) — Microsoft Support for Windows Server 2008 R2 Premium Assurance	CVE-2024-49118	Remote Code Execution	Critical	No	No	2
			CVE-2024-49082	Information Disclosure	Important	No	No	2
			CVE-2024-49102	Remote Code Execution	Important	No	No	2
			CVE-2024-49089	Remote Code Execution	Important	No	No	2
			CVE-2024-49113	Denial of Service	Important	No	No	2
			CVE-2024-49105	Remote Code Execution	Critical	No	No	2
			CVE-2024-49090	Elevation of Privilege	Important	No	No	1
			CVE-2024-49126	Remote Code Execution	Critical	No	No	2
			CVE-2024-49072	Elevation of Privilege	Important	No	No	2
			CVE-2024-49096	Denial of Service	Important	No	No	2
			CVE-2024-49112	Remote Code Execution	Critical	No	No	2
			CVE-2024-49125	Remote Code Execution	Important	No	No	2
			CVE-2024-49127	Remote Code Execution	Critical	No	No	2
			CVE-2024-49121	Denial of Service	Important	No	No	2
			CVE-2024-49085	Remote Code Execution	Important	No	No	2

			CVE-2024-49124	Remote Code Execution	Critical	No	No	2
			CVE-2024-49086	Remote Code Execution	Important	No	No	2
			CVE-2024-49122	Remote Code Execution	Critical	No	No	1
			CVE-2024-49138	Elevation of Privilege	Important	Yes	Yes	0
			CVE-2024-49080	Remote Code Execution	Important	No	No	2
			CVE-2024-49088	Elevation of Privilege	Important	No	No	1
			CVE-2024-49084	Elevation of Privilege	Important	No	No	2
			CVE-2024-49104	Remote Code Execution	Important	No	No	2
5048710	高危	December 10, 2024—KB5048710 (Monthly Rollup) – Microsoft Support for Windows Server 2008 Premium Assurance	CVE-2024-49118	Remote Code Execution	Critical	No	No	2
			CVE-2024-49082	Information Disclosure	Important	No	No	2
			CVE-2024-49102	Remote Code Execution	Important	No	No	2
			CVE-2024-49089	Remote Code Execution	Important	No	No	2
			CVE-2024-49113	Denial of Service	Important	No	No	2
			CVE-2024-49090	Elevation of Privilege	Important	No	No	1
			CVE-2024-49126	Remote Code Execution	Critical	No	No	2
			CVE-2024-49072	Elevation of Privilege	Important	No	No	2
			CVE-2024-49096	Denial of Service	Important	No	No	2
			CVE-2024-49112	Remote Code Execution	Critical	No	No	2
			CVE-2024-49125	Remote Code Execution	Important	No	No	2
			CVE-2024-49127	Remote Code Execution	Critical	No	No	2

			CVE-2024-49121	Denial of Service	Important	No	No	2
			CVE-2024-49085	Remote Code Execution	Important	No	No	2
			CVE-2024-49124	Remote Code Execution	Critical	No	No	2
			CVE-2024-49086	Remote Code Execution	Important	No	No	2
			CVE-2024-49122	Remote Code Execution	Critical	No	No	1
			CVE-2024-49138	Elevation of Privilege	Important	Yes	Yes	0
			CVE-2024-49080	Remote Code Execution	Important	No	No	2
			CVE-2024-49088	Elevation of Privilege	Important	No	No	1
			CVE-2024-49084	Elevation of Privilege	Important	No	No	2
			CVE-2024-49104	Remote Code Execution	Important	No	No	2
5048652	高危	December 10, 2024—KB5048652 (OS Builds 19044.5247 and 19045.5247) – Microsoft Support for Windows 10 Enterprise LTSC 2021, Windows 10	CVE-2024-49118	Remote Code Execution	Critical	No	No	2
			CVE-2024-49092	Elevation of Privilege	Important	No	No	2
			CVE-2024-49132	Remote Code Execution	Critical	No	No	2
			CVE-2024-49082	Information Disclosure	Important	No	No	2
			CVE-2024-49083	Elevation of Privilege	Important	No	No	2
			CVE-2024-49123	Remote Code Execution	Critical	No	No	2
			CVE-2024-49102	Remote Code Execution	Important	No	No	2
			CVE-2024-49089	Remote Code Execution	Important	No	No	2
			CVE-2024-49107	Elevation of Privilege	Important	No	No	2
			CVE-2024-49103	Information Disclosure	Important	No	No	2

		IoT Enterprise LTSC 2021, Windows 10, version 22H2, all editions	CVE-2024-49113	Denial of Service	Important	No	No	2
			CVE-2024-49105	Remote Code Execution	Critical	No	No	2
			CVE-2024-49111	Elevation of Privilege	Important	No	No	2
			CVE-2024-49090	Elevation of Privilege	Important	No	No	1
			CVE-2024-49126	Remote Code Execution	Critical	No	No	2
			CVE-2024-49072	Elevation of Privilege	Important	No	No	2
			CVE-2024-49096	Denial of Service	Important	No	No	2
			CVE-2024-49074	Elevation of Privilege	Important	No	No	2
			CVE-2024-49099	Information Disclosure	Important	No	No	2
			CVE-2024-49079	Remote Code Execution	Important	No	No	2
			CVE-2024-49095	Elevation of Privilege	Important	No	No	2
			CVE-2024-49114	Elevation of Privilege	Important	No	No	1
			CVE-2024-49112	Remote Code Execution	Critical	No	No	2
			CVE-2024-49098	Information Disclosure	Important	No	No	2
			CVE-2024-49127	Remote Code Execution	Critical	No	No	2
			CVE-2024-49121	Denial of Service	Important	No	No	2
			CVE-2024-49075	Denial of Service	Important	No	No	2
			CVE-2024-49124	Remote Code Execution	Critical	No	No	2
			CVE-2024-49077	Elevation of Privilege	Important	No	No	2
			CVE-2024-49122	Remote Code Execution	Critical	No	No	1

			CVE-2024-49101	Elevation of Privilege	Important	No	No	2
			CVE-2024-49110	Elevation of Privilege	Important	No	No	2
			CVE-2024-49138	Elevation of Privilege	Important	Yes	Yes	0
			CVE-2024-49073	Elevation of Privilege	Important	No	No	2
			CVE-2024-49080	Remote Code Execution	Important	No	No	2
			CVE-2024-49081	Elevation of Privilege	Important	No	No	2
			CVE-2024-49088	Elevation of Privilege	Important	No	No	1
			CVE-2024-49084	Elevation of Privilege	Important	No	No	2
			CVE-2024-49104	Remote Code Execution	Important	No	No	2
			CVE-2024-49087	Information Disclosure	Important	No	No	2
			CVE-2024-49094	Elevation of Privilege	Important	No	No	2
			CVE-2024-49078	Elevation of Privilege	Important	No	No	2
			CVE-2024-49109	Elevation of Privilege	Important	No	No	2
			CVE-2024-49097	Elevation of Privilege	Important	No	No	2
			CVE-2024-49076	Elevation of Privilege	Important	No	No	2
5048735	高危	December 10, 2024—KB5048735 (Monthly Rollup) — Microsoft	CVE-2024-49118	Remote Code Execution	Critical	No	No	2
			CVE-2024-49082	Information Disclosure	Important	No	No	2
			CVE-2024-49102	Remote Code Execution	Important	No	No	2
			CVE-2024-49089	Remote Code Execution	Important	No	No	2
			CVE-2024-49113	Denial of Service	Important	No	No	2

		Support for Windows Server 2012 R2 ESU	CVE-2024-49105	Remote Code Execution	Critical	No	No	2
			CVE-2024-49090	Elevation of Privilege	Important	No	No	1
			CVE-2024-49128	Remote Code Execution	Critical	No	No	2
			CVE-2024-49126	Remote Code Execution	Critical	No	No	2
			CVE-2024-49072	Elevation of Privilege	Important	No	No	2
			CVE-2024-49096	Denial of Service	Important	No	No	2
			CVE-2024-49120	Remote Code Execution	Critical	No	No	2
			CVE-2024-49091	Remote Code Execution	Important	No	No	2
			CVE-2024-49079	Remote Code Execution	Important	No	No	2
			CVE-2024-49112	Remote Code Execution	Critical	No	No	2
			CVE-2024-49125	Remote Code Execution	Important	No	No	2
			CVE-2024-49127	Remote Code Execution	Critical	No	No	2
			CVE-2024-49121	Denial of Service	Important	No	No	2
			CVE-2024-49085	Remote Code Execution	Important	No	No	2
			CVE-2024-49124	Remote Code Execution	Critical	No	No	2
			CVE-2024-49086	Remote Code Execution	Important	No	No	2
			CVE-2024-49122	Remote Code Execution	Critical	No	No	1
			CVE-2024-49138	Elevation of Privilege	Important	Yes	Yes	0
			CVE-2024-49080	Remote Code Execution	Important	No	No	2
			CVE-2024-49088	Elevation of Privilege	Important	No	No	1

			CVE-2024-49084	Elevation of Privilege	Important	No	No	2
			CVE-2024-49129	Denial of Service	Important	No	No	2
			CVE-2024-49104	Remote Code Execution	Important	No	No	2
5048667	高危	December 10, 2024—KB5048667 (OS Build 26100.2605) – Microsoft Support for Windows 11 version 24H2, all editions	CVE-2024-49118	Remote Code Execution	Critical	No	No	2
			CVE-2024-49092	Elevation of Privilege	Important	No	No	2
			CVE-2024-49132	Remote Code Execution	Critical	No	No	2
			CVE-2024-49082	Information Disclosure	Important	No	No	2
			CVE-2024-49108	Remote Code Execution	Critical	No	No	2
			CVE-2024-49083	Elevation of Privilege	Important	No	No	2
			CVE-2024-49123	Remote Code Execution	Critical	No	No	2
			CVE-2024-49102	Remote Code Execution	Important	No	No	2
			CVE-2024-49089	Remote Code Execution	Important	No	No	2
			CVE-2024-49116	Remote Code Execution	Critical	No	No	2
			CVE-2024-49115	Remote Code Execution	Critical	No	No	2
			CVE-2024-49107	Elevation of Privilege	Important	No	No	2
			CVE-2024-49103	Information Disclosure	Important	No	No	2
			CVE-2024-49113	Denial of Service	Important	No	No	2
			CVE-2024-49105	Remote Code Execution	Critical	No	No	2
			CVE-2024-49111	Elevation of Privilege	Important	No	No	2
			CVE-2024-49090	Elevation of Privilege	Important	No	No	1

			CVE-2024-49128	Remote Code Execution	Critical	No	No	2
			CVE-2024-49126	Remote Code Execution	Critical	No	No	2
			CVE-2024-49072	Elevation of Privilege	Important	No	No	2
			CVE-2024-49096	Denial of Service	Important	No	No	2
			CVE-2024-49120	Remote Code Execution	Critical	No	No	2
			CVE-2024-49091	Remote Code Execution	Important	No	No	2
			CVE-2024-49099	Information Disclosure	Important	No	No	2
			CVE-2024-49079	Remote Code Execution	Important	No	No	2
			CVE-2024-49095	Elevation of Privilege	Important	No	No	2
			CVE-2024-49114	Elevation of Privilege	Important	No	No	1
			CVE-2024-49112	Remote Code Execution	Critical	No	No	2
			CVE-2024-49125	Remote Code Execution	Important	No	No	2
			CVE-2024-49127	Remote Code Execution	Critical	No	No	2
			CVE-2024-49098	Information Disclosure	Important	No	No	2
			CVE-2024-49121	Denial of Service	Important	No	No	2
			CVE-2024-49117	Remote Code Execution	Critical	No	No	2
			CVE-2024-49085	Remote Code Execution	Important	No	No	2
			CVE-2024-49075	Denial of Service	Important	No	No	2
			CVE-2024-49124	Remote Code Execution	Critical	No	No	2
			CVE-2024-49077	Elevation of Privilege	Important	No	No	2

			CVE-2024-49086	Remote Code Execution	Important	No	No	2
			CVE-2024-49122	Remote Code Execution	Critical	No	No	1
			CVE-2024-49101	Elevation of Privilege	Important	No	No	2
			CVE-2024-49110	Elevation of Privilege	Important	No	No	2
			CVE-2024-49138	Elevation of Privilege	Important	Yes	Yes	0
			CVE-2024-49073	Elevation of Privilege	Important	No	No	2
			CVE-2024-49093	Elevation of Privilege	Important	No	No	1
			CVE-2024-49088	Elevation of Privilege	Important	No	No	1
			CVE-2024-49081	Elevation of Privilege	Important	No	No	2
			CVE-2024-49080	Remote Code Execution	Important	No	No	2
			CVE-2024-49084	Elevation of Privilege	Important	No	No	2
			CVE-2024-49129	Denial of Service	Important	No	No	2
			CVE-2024-49104	Remote Code Execution	Important	No	No	2
			CVE-2024-49106	Remote Code Execution	Critical	No	No	2
			CVE-2024-49087	Information Disclosure	Important	No	No	2
			CVE-2024-49119	Remote Code Execution	Critical	No	No	2
			CVE-2024-49094	Elevation of Privilege	Important	No	No	2
			CVE-2024-49078	Elevation of Privilege	Important	No	No	2
			CVE-2024-49109	Elevation of Privilege	Important	No	No	2
			CVE-2024-49097	Elevation of Privilege	Important	No	No	2

			CVE-2024-49076	Elevation of Privilege	Important	No	No	2
5048699	高危	December 10, 2024—KB5048699 (Monthly Rollup) – Microsoft Support for Windows Server 2012 ESU	CVE-2024-49118	Remote Code Execution	Critical	No	No	2
			CVE-2024-49082	Information Disclosure	Important	No	No	2
			CVE-2024-49102	Remote Code Execution	Important	No	No	2
			CVE-2024-49089	Remote Code Execution	Important	No	No	2
			CVE-2024-49113	Denial of Service	Important	No	No	2
			CVE-2024-49105	Remote Code Execution	Critical	No	No	2
			CVE-2024-49090	Elevation of Privilege	Important	No	No	1
			CVE-2024-49128	Remote Code Execution	Critical	No	No	2
			CVE-2024-49126	Remote Code Execution	Critical	No	No	2
			CVE-2024-49072	Elevation of Privilege	Important	No	No	2
			CVE-2024-49096	Denial of Service	Important	No	No	2
			CVE-2024-49120	Remote Code Execution	Critical	No	No	2
			CVE-2024-49091	Remote Code Execution	Important	No	No	2
			CVE-2024-49079	Remote Code Execution	Important	No	No	2
			CVE-2024-49112	Remote Code Execution	Critical	No	No	2
			CVE-2024-49125	Remote Code Execution	Important	No	No	2
			CVE-2024-49127	Remote Code Execution	Critical	No	No	2
			CVE-2024-49121	Denial of Service	Important	No	No	2
			CVE-2024-49085	Remote Code Execution	Important	No	No	2

			CVE-2024-49124	Remote Code Execution	Critical	No	No	2
			CVE-2024-49086	Remote Code Execution	Important	No	No	2
			CVE-2024-49122	Remote Code Execution	Critical	No	No	1
			CVE-2024-49138	Elevation of Privilege	Important	Yes	Yes	0
			CVE-2024-49080	Remote Code Execution	Important	No	No	2
			CVE-2024-49088	Elevation of Privilege	Important	No	No	1
			CVE-2024-49084	Elevation of Privilege	Important	No	No	2
			CVE-2024-49129	Denial of Service	Important	No	No	2
			CVE-2024-49104	Remote Code Execution	Important	No	No	2
5048671	高危	December 10, 2024—KB5048671 (OS Build 14393.7606) – Microsoft Support for Windows 10, version 1607, all editions, Windows Server 2016,	CVE-2024-49118	Remote Code Execution	Critical	No	No	2
			CVE-2024-49082	Information Disclosure	Important	No	No	2
			CVE-2024-49108	Remote Code Execution	Critical	No	No	2
			CVE-2024-49102	Remote Code Execution	Important	No	No	2
			CVE-2024-49089	Remote Code Execution	Important	No	No	2
			CVE-2024-49116	Remote Code Execution	Critical	No	No	2
			CVE-2024-49115	Remote Code Execution	Critical	No	No	2
			CVE-2024-49107	Elevation of Privilege	Important	No	No	2
			CVE-2024-49113	Denial of Service	Important	No	No	2
			CVE-2024-49105	Remote Code Execution	Critical	No	No	2
			CVE-2024-49090	Elevation of Privilege	Important	No	No	1

		all editions	CVE-2024-49128	Remote Code Execution	Critical	No	No	2
			CVE-2024-49126	Remote Code Execution	Critical	No	No	2
			CVE-2024-49072	Elevation of Privilege	Important	No	No	2
			CVE-2024-49096	Denial of Service	Important	No	No	2
			CVE-2024-49120	Remote Code Execution	Critical	No	No	2
			CVE-2024-49091	Remote Code Execution	Important	No	No	2
			CVE-2024-49079	Remote Code Execution	Important	No	No	2
			CVE-2024-49112	Remote Code Execution	Critical	No	No	2
			CVE-2024-49125	Remote Code Execution	Important	No	No	2
			CVE-2024-49127	Remote Code Execution	Critical	No	No	2
			CVE-2024-49121	Denial of Service	Important	No	No	2
			CVE-2024-49085	Remote Code Execution	Important	No	No	2
			CVE-2024-49124	Remote Code Execution	Critical	No	No	2
			CVE-2024-49086	Remote Code Execution	Important	No	No	2
			CVE-2024-49122	Remote Code Execution	Critical	No	No	1
			CVE-2024-49138	Elevation of Privilege	Important	Yes	Yes	0
			CVE-2024-49080	Remote Code Execution	Important	No	No	2
			CVE-2024-49088	Elevation of Privilege	Important	No	No	1
			CVE-2024-49084	Elevation of Privilege	Important	No	No	2
			CVE-2024-49129	Denial of Service	Important	No	No	2

			CVE-2024-49104	Remote Code Execution	Important	No	No	2
			CVE-2024-49106	Remote Code Execution	Critical	No	No	2
			CVE-2024-49119	Remote Code Execution	Critical	No	No	2
5048661	高危	December 10, 2024—KB5048661 (OS Build 17763.6659) – Microsoft Support for Win 10 Ent LTSC 2019, Win 10 IoT Ent LTSC 2019, Windows 10 IoT Core LTSC, Windows Server 2019	CVE-2024-49118	Remote Code Execution	Critical	No	No	2
			CVE-2024-49092	Elevation of Privilege	Important	No	No	2
			CVE-2024-49132	Remote Code Execution	Critical	No	No	2
			CVE-2024-49082	Information Disclosure	Important	No	No	2
			CVE-2024-49108	Remote Code Execution	Critical	No	No	2
			CVE-2024-49083	Elevation of Privilege	Important	No	No	2
			CVE-2024-49123	Remote Code Execution	Critical	No	No	2
			CVE-2024-49102	Remote Code Execution	Important	No	No	2
			CVE-2024-49089	Remote Code Execution	Important	No	No	2
			CVE-2024-49116	Remote Code Execution	Critical	No	No	2
			CVE-2024-49115	Remote Code Execution	Critical	No	No	2
			CVE-2024-49107	Elevation of Privilege	Important	No	No	2
			CVE-2024-49103	Information Disclosure	Important	No	No	2
			CVE-2024-49113	Denial of Service	Important	No	No	2
			CVE-2024-49105	Remote Code Execution	Critical	No	No	2
			CVE-2024-49111	Elevation of Privilege	Important	No	No	2
			CVE-2024-49090	Elevation of Privilege	Important	No	No	1

			CVE-2024-49128	Remote Code Execution	Critical	No	No	2
			CVE-2024-49126	Remote Code Execution	Critical	No	No	2
			CVE-2024-49072	Elevation of Privilege	Important	No	No	2
			CVE-2024-49096	Denial of Service	Important	No	No	2
			CVE-2024-49120	Remote Code Execution	Critical	No	No	2
			CVE-2024-49074	Elevation of Privilege	Important	No	No	2
			CVE-2024-49091	Remote Code Execution	Important	No	No	2
			CVE-2024-49099	Information Disclosure	Important	No	No	2
			CVE-2024-49079	Remote Code Execution	Important	No	No	2
			CVE-2024-49095	Elevation of Privilege	Important	No	No	2
			CVE-2024-49114	Elevation of Privilege	Important	No	No	1
			CVE-2024-49112	Remote Code Execution	Critical	No	No	2
			CVE-2024-49125	Remote Code Execution	Important	No	No	2
			CVE-2024-49127	Remote Code Execution	Critical	No	No	2
			CVE-2024-49098	Information Disclosure	Important	No	No	2
			CVE-2024-49121	Denial of Service	Important	No	No	2
			CVE-2024-49085	Remote Code Execution	Important	No	No	2
			CVE-2024-49075	Denial of Service	Important	No	No	2
			CVE-2024-49124	Remote Code Execution	Critical	No	No	2
			CVE-2024-49077	Elevation of Privilege	Important	No	No	2

			CVE-2024-49086	Remote Code Execution	Important	No	No	2
			CVE-2024-49122	Remote Code Execution	Critical	No	No	1
			CVE-2024-49101	Elevation of Privilege	Important	No	No	2
			CVE-2024-49110	Elevation of Privilege	Important	No	No	2
			CVE-2024-49138	Elevation of Privilege	Important	Yes	Yes	0
			CVE-2024-49073	Elevation of Privilege	Important	No	No	2
			CVE-2024-49088	Elevation of Privilege	Important	No	No	1
			CVE-2024-49081	Elevation of Privilege	Important	No	No	2
			CVE-2024-49080	Remote Code Execution	Important	No	No	2
			CVE-2024-49084	Elevation of Privilege	Important	No	No	2
			CVE-2024-49129	Denial of Service	Important	No	No	2
			CVE-2024-49104	Remote Code Execution	Important	No	No	2
			CVE-2024-49106	Remote Code Execution	Critical	No	No	2
			CVE-2024-49087	Information Disclosure	Important	No	No	2
			CVE-2024-49119	Remote Code Execution	Critical	No	No	2
			CVE-2024-49094	Elevation of Privilege	Important	No	No	2
			CVE-2024-49078	Elevation of Privilege	Important	No	No	2
			CVE-2024-49109	Elevation of Privilege	Important	No	No	2
			CVE-2024-49097	Elevation of Privilege	Important	No	No	2
			CVE-2024-49076	Elevation of Privilege	Important	No	No	2

5048744	高危	December 10, 2024—KB5048744 (Security-only update) – Microsoft Support for Windows Server 2008 Premium Assurance	CVE-2024-49118	Remote Code Execution	Critical	No	No	2
			CVE-2024-49082	Information Disclosure	Important	No	No	2
			CVE-2024-49102	Remote Code Execution	Important	No	No	2
			CVE-2024-49089	Remote Code Execution	Important	No	No	2
			CVE-2024-49113	Denial of Service	Important	No	No	2
			CVE-2024-49090	Elevation of Privilege	Important	No	No	1
			CVE-2024-49126	Remote Code Execution	Critical	No	No	2
			CVE-2024-49072	Elevation of Privilege	Important	No	No	2
			CVE-2024-49096	Denial of Service	Important	No	No	2
			CVE-2024-49112	Remote Code Execution	Critical	No	No	2
			CVE-2024-49125	Remote Code Execution	Important	No	No	2
			CVE-2024-49127	Remote Code Execution	Critical	No	No	2
			CVE-2024-49121	Denial of Service	Important	No	No	2
			CVE-2024-49085	Remote Code Execution	Important	No	No	2
			CVE-2024-49124	Remote Code Execution	Critical	No	No	2
			CVE-2024-49086	Remote Code Execution	Important	No	No	2
			CVE-2024-49122	Remote Code Execution	Critical	No	No	1
			CVE-2024-49138	Elevation of Privilege	Important	Yes	Yes	0
			CVE-2024-49080	Remote Code Execution	Important	No	No	2
			CVE-2024-49088	Elevation of Privilege	Important	No	No	1

			CVE-2024-49084	Elevation of Privilege	Important	No	No	2
			CVE-2024-49104	Remote Code Execution	Important	No	No	2
5048676	高危	December 10, 2024—KB5048676 (Security-only update) – Microsoft Support for Windows Server 2008 R2 Premium Assurance	CVE-2024-49118	Remote Code Execution	Critical	No	No	2
			CVE-2024-49082	Information Disclosure	Important	No	No	2
			CVE-2024-49102	Remote Code Execution	Important	No	No	2
			CVE-2024-49089	Remote Code Execution	Important	No	No	2
			CVE-2024-49113	Denial of Service	Important	No	No	2
			CVE-2024-49105	Remote Code Execution	Critical	No	No	2
			CVE-2024-49090	Elevation of Privilege	Important	No	No	1
			CVE-2024-49126	Remote Code Execution	Critical	No	No	2
			CVE-2024-49072	Elevation of Privilege	Important	No	No	2
			CVE-2024-49096	Denial of Service	Important	No	No	2
			CVE-2024-49112	Remote Code Execution	Critical	No	No	2
			CVE-2024-49125	Remote Code Execution	Important	No	No	2
			CVE-2024-49127	Remote Code Execution	Critical	No	No	2
			CVE-2024-49121	Denial of Service	Important	No	No	2
			CVE-2024-49085	Remote Code Execution	Important	No	No	2
			CVE-2024-49124	Remote Code Execution	Critical	No	No	2
			CVE-2024-49086	Remote Code Execution	Important	No	No	2
			CVE-2024-49122	Remote Code Execution	Critical	No	No	1

			CVE-2024-49138	Elevation of Privilege	Important	Yes	Yes	0
			CVE-2024-49080	Remote Code Execution	Important	No	No	2
			CVE-2024-49088	Elevation of Privilege	Important	No	No	1
			CVE-2024-49084	Elevation of Privilege	Important	No	No	2
			CVE-2024-49104	Remote Code Execution	Important	No	No	2
5048685	高危	December 10, 2024—KB5048685 (OS Builds 22621.46 02 and 22631.46 02) – Microsoft Support for Windows 11 Enterprise and Education, version 22H2, Windows 11 version 23H2, all editions	CVE-2024-49118	Remote Code Execution	Critical	No	No	2
			CVE-2024-49092	Elevation of Privilege	Important	No	No	2
			CVE-2024-49132	Remote Code Execution	Critical	No	No	2
			CVE-2024-49082	Information Disclosure	Important	No	No	2
			CVE-2024-49083	Elevation of Privilege	Important	No	No	2
			CVE-2024-49123	Remote Code Execution	Critical	No	No	2
			CVE-2024-49102	Remote Code Execution	Important	No	No	2
			CVE-2024-49089	Remote Code Execution	Important	No	No	2
			CVE-2024-49107	Elevation of Privilege	Important	No	No	2
			CVE-2024-49103	Information Disclosure	Important	No	No	2
			CVE-2024-49113	Denial of Service	Important	No	No	2
			CVE-2024-49105	Remote Code Execution	Critical	No	No	2
			CVE-2024-49111	Elevation of Privilege	Important	No	No	2
			CVE-2024-49090	Elevation of Privilege	Important	No	No	1
			CVE-2024-49126	Remote Code Execution	Critical	No	No	2

			CVE-2024-49072	Elevation of Privilege	Important	No	No	2
			CVE-2024-49096	Denial of Service	Important	No	No	2
			CVE-2024-49099	Information Disclosure	Important	No	No	2
			CVE-2024-49079	Remote Code Execution	Important	No	No	2
			CVE-2024-49095	Elevation of Privilege	Important	No	No	2
			CVE-2024-49114	Elevation of Privilege	Important	No	No	1
			CVE-2024-49112	Remote Code Execution	Critical	No	No	2
			CVE-2024-49098	Information Disclosure	Important	No	No	2
			CVE-2024-49127	Remote Code Execution	Critical	No	No	2
			CVE-2024-49121	Denial of Service	Important	No	No	2
			CVE-2024-49117	Remote Code Execution	Critical	No	No	2
			CVE-2024-49075	Denial of Service	Important	No	No	2
			CVE-2024-49124	Remote Code Execution	Critical	No	No	2
			CVE-2024-49077	Elevation of Privilege	Important	No	No	2
			CVE-2024-49122	Remote Code Execution	Critical	No	No	1
			CVE-2024-49101	Elevation of Privilege	Important	No	No	2
			CVE-2024-49110	Elevation of Privilege	Important	No	No	2
			CVE-2024-49138	Elevation of Privilege	Important	Yes	Yes	0
			CVE-2024-49073	Elevation of Privilege	Important	No	No	2
			CVE-2024-49080	Remote Code Execution	Important	No	No	2

			CVE-2024-49081	Elevation of Privilege	Important	No	No	2
			CVE-2024-49088	Elevation of Privilege	Important	No	No	1
			CVE-2024-49084	Elevation of Privilege	Important	No	No	2
			CVE-2024-49104	Remote Code Execution	Important	No	No	2
			CVE-2024-49087	Information Disclosure	Important	No	No	2
			CVE-2024-49094	Elevation of Privilege	Important	No	No	2
			CVE-2024-49078	Elevation of Privilege	Important	No	No	2
			CVE-2024-49109	Elevation of Privilege	Important	No	No	2
			CVE-2024-49097	Elevation of Privilege	Important	No	No	2
			CVE-2024-49076	Elevation of Privilege	Important	No	No	2
5048654	高危	December 10, 2024—KB5048654 (OS Build 20348.2966) – Microsoft Support for Windows Server 2022	CVE-2024-49118	Remote Code Execution	Critical	No	No	2
			CVE-2024-49132	Remote Code Execution	Critical	No	No	2
			CVE-2024-49082	Information Disclosure	Important	No	No	2
			CVE-2024-49108	Remote Code Execution	Critical	No	No	2
			CVE-2024-49123	Remote Code Execution	Critical	No	No	2
			CVE-2024-49102	Remote Code Execution	Important	No	No	2
			CVE-2024-49089	Remote Code Execution	Important	No	No	2
			CVE-2024-49116	Remote Code Execution	Critical	No	No	2
			CVE-2024-49115	Remote Code Execution	Critical	No	No	2
			CVE-2024-49107	Elevation of Privilege	Important	No	No	2

			CVE-2024-49113	Denial of Service	Important	No	No	2
			CVE-2024-49105	Remote Code Execution	Critical	No	No	2
			CVE-2024-49090	Elevation of Privilege	Important	No	No	1
			CVE-2024-49128	Remote Code Execution	Critical	No	No	2
			CVE-2024-49126	Remote Code Execution	Critical	No	No	2
			CVE-2024-49072	Elevation of Privilege	Important	No	No	2
			CVE-2024-49096	Denial of Service	Important	No	No	2
			CVE-2024-49120	Remote Code Execution	Critical	No	No	2
			CVE-2024-49091	Remote Code Execution	Important	No	No	2
			CVE-2024-49079	Remote Code Execution	Important	No	No	2
			CVE-2024-49095	Elevation of Privilege	Important	No	No	2
			CVE-2024-49114	Elevation of Privilege	Important	No	No	1
			CVE-2024-49112	Remote Code Execution	Critical	No	No	2
			CVE-2024-49125	Remote Code Execution	Important	No	No	2
			CVE-2024-49127	Remote Code Execution	Critical	No	No	2
			CVE-2024-49121	Denial of Service	Important	No	No	2
			CVE-2024-49117	Remote Code Execution	Critical	No	No	2
			CVE-2024-49085	Remote Code Execution	Important	No	No	2
			CVE-2024-49075	Denial of Service	Important	No	No	2
			CVE-2024-49124	Remote Code Execution	Critical	No	No	2

			CVE-2024-49086	Remote Code Execution	Important	No	No	2
			CVE-2024-49122	Remote Code Execution	Critical	No	No	1
			CVE-2024-49138	Elevation of Privilege	Important	Yes	Yes	0
			CVE-2024-49080	Remote Code Execution	Important	No	No	2
			CVE-2024-49088	Elevation of Privilege	Important	No	No	1
			CVE-2024-49084	Elevation of Privilege	Important	No	No	2
			CVE-2024-49129	Denial of Service	Important	No	No	2
			CVE-2024-49104	Remote Code Execution	Important	No	No	2
			CVE-2024-49106	Remote Code Execution	Critical	No	No	2
			CVE-2024-49119	Remote Code Execution	Critical	No	No	2
			CVE-2024-49097	Elevation of Privilege	Important	No	No	2
			CVE-2024-49076	Elevation of Privilege	Important	No	No	2
5048703	高危	December 10, 2024—KB5048703 (OS Build 10240.20857) – Microsoft Support for Windows 10	CVE-2024-49118	Remote Code Execution	Critical	No	No	2
			CVE-2024-49082	Information Disclosure	Important	No	No	2
			CVE-2024-49102	Remote Code Execution	Important	No	No	2
			CVE-2024-49089	Remote Code Execution	Important	No	No	2
			CVE-2024-49107	Elevation of Privilege	Important	No	No	2
			CVE-2024-49113	Denial of Service	Important	No	No	2
			CVE-2024-49105	Remote Code Execution	Critical	No	No	2
			CVE-2024-49090	Elevation of Privilege	Important	No	No	1

			CVE-2024-49126	Remote Code Execution	Critical	No	No	2
			CVE-2024-49072	Elevation of Privilege	Important	No	No	2
			CVE-2024-49096	Denial of Service	Important	No	No	2
			CVE-2024-49079	Remote Code Execution	Important	No	No	2
			CVE-2024-49112	Remote Code Execution	Critical	No	No	2
			CVE-2024-49127	Remote Code Execution	Critical	No	No	2
			CVE-2024-49121	Denial of Service	Important	No	No	2
			CVE-2024-49124	Remote Code Execution	Critical	No	No	2
			CVE-2024-49122	Remote Code Execution	Critical	No	No	1
			CVE-2024-49138	Elevation of Privilege	Important	Yes	Yes	0
			CVE-2024-49080	Remote Code Execution	Important	No	No	2
			CVE-2024-49088	Elevation of Privilege	Important	No	No	1
			CVE-2024-49084	Elevation of Privilege	Important	No	No	2
			CVE-2024-49104	Remote Code Execution	Important	No	No	2

本月微软发布的软件安全更新补丁共 8 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
5002661	高危	Description of the security update for Office 2016: December 10, 2024 (KB5002661) – Microsoft Support	CVE-2024-49065	Remote Code Execution	Important	No	No	2
			CVE-2024-43600	Elevation of Privilege	Important	No	No	2
5002544	高危	Description of the security update for SharePoint Enterprise Server 2016 Language Pack: December 10, 2024 (KB5002544) – Microsoft Support	CVE-2024-49068	Elevation of Privilege	Important	No	No	2
			CVE-2024-49070	Remote Code Execution	Important	No	No	1
			CVE-2024-49064	Information Disclosure	Important	No	No	2
			CVE-2024-49062	Information Disclosure	Important	No	No	2
5002641	高危	Description of the security update for Access 2016: December 10, 2024 (KB5002641)	CVE-2024-49142	Remote Code Execution	Important	No	No	2

		- Microsoft Support						
4475587	高危	Description of the security update for Office 2016: December 10, 2024 (KB4475587) - Microsoft Support	CVE-2024-43600	Elevation of Privilege	Important	No	No	2
			CVE-2024-49059	Elevation of Privilege	Important	No	No	2
5002659	高危	Description of the security update for SharePoint Enterprise Server 2016: December 10, 2024 (KB5002659) - Microsoft Support	CVE-2024-49064	Information Disclosure	Important	No	No	2
			CVE-2024-49070	Remote Code Execution	Important	No	No	1
			CVE-2024-49065	Remote Code Execution	Important	No	No	2
			CVE-2024-49068	Elevation of Privilege	Important	No	No	2
			CVE-2024-49062	Information Disclosure	Important	No	No	2
5002652	高危	Description of the security update for Project 2016: December 10, 2024 (KB5002652) - Microsoft Support	ADV240002	Defense in Depth	Moderate			4
5002660	高危	Description of the security update for Excel 2016: December 10, 2024	CVE-2024-49069	Remote Code Execution	Important	No	No	2

		(KB5002660) - Microsoft Support						
2920716	高危	Description of the security update for Office 2016: December 10, 2024 (KB2920716) - Microsoft Support	CVE-2024-43600	Elevation of Privilege	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>