奇安信集团 2025 年 06 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

2025 年 05 月 14 日

目 录

文档信息

文档名称	奇安信集团 2025 年 06 月补丁库更新通告		
文档编号	Qi An Xin Group-MSPatch-2025-0601		
发布日期	2025-06-11	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:2025.06.11.1,V10版本:2025.06.11.1000)已发布，本次更新推送了22个微软安全补丁，修复了53个安全漏洞，其中8个微软官方评级为“严重(Critical)”，45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 12 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
5060526	CVE-2025-32714	Elevation of Privilege	Important	No	No	Exploitation More Likely
5060531						
5060999						
5060998						
5061072						
5061018						
5061026						
5060533						
5061078						
5061036						
5061010						
5060842						
5061059						
5060526	CVE-2025-33071	Remote Code Execution	Critical	No	No	Exploitation More Likely
5060531						
5061018						
5061010						
5060842						
5061059						
5060526	CVE-2025-33053	Remote Code Execution	Important	No	Yes	Exploitation Detected
5060531						
5060999						
5060998						
5061018						
5061026						
5060533						
5061078						
5061010						

5060842						
5060996						
5061059						
5060526	CVE-2025-29828	Remote Code Execution	Critical	No	No	Exploitation Less Likely
5060999						
5060842						
5060526	CVE-2025-32713	Elevation of Privilege	Important	No	No	Exploitation More Likely
5060531						
5060999						
5060998						
5061072						
5061018						
5061026						
5060533						
5061078						
5061036						
5061010						
5060842						
5061059						
5060526	CVE-2025-33073	Elevation of Privilege	Important	Yes	No	Exploitation Less Likely
5060531						
5060999						
5060998						
5061072						
5061018						
5061026						
5060533						
5061078						
5061036						
5061010						
5060842						
5061059						
5060526	CVE-2025-33070	Elevation of Privilege	Critical	No	No	Exploitation More Likely
5060531						
5060999						
5060998						
5061018						
5060533						
5061078						
5061036						
5061010						

5060842 5061059						
5002732	CVE-2025-47172	Remote Code Execution	Critical	No	No	Exploitation Less Likely
5002616	CVE-2025-47167	Remote Code Execution	Critical	No	No	Exploitation More Likely
5002730	CVE-2025-47162	Remote Code Execution	Critical	No	No	Exploitation More Likely
5002730	CVE-2025-47164	Remote Code Execution	Critical	No	No	Exploitation More Likely
5002730	CVE-2025-47953	Remote Code Execution	Critical	No	No	Exploitation Less Likely

第3章 已知问题和特殊调整

本月暂无已知问题和特殊调整。

第4章 漏洞补丁详细列表

本月微软发布的系统安全更新补丁共 13 个，详细列表如下：

KBID	奇安信集团级别	补丁名称	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
5060526	高危	June 10, 2025—KB5060526 (OS Build 20348.3807) - Microsoft Support for Windows Server 2022	CVE-2025-33060	Information Disclosure	Important	No	No	3
			CVE-2025-32722	Information Disclosure	Important	No	No	2
			CVE-2025-32714	Elevation of Privilege	Important	No	No	1
			CVE-2025-33075	Elevation of Privilege	Important	No	No	2
			CVE-2025-33058	Information Disclosure	Important	No	No	2
			CVE-2025-32715	Information Disclosure	Important	No	No	2
			CVE-2025-32719	Information Disclosure	Important	No	No	3
			CVE-2025-47160	Security Feature Bypass	Important	No	No	2
			CVE-2025-32720	Information Disclosure	Important	No	No	3
			CVE-2025-3052	Security Feature Bypass	Important	No	No	2
			CVE-2025-33071	Remote Code Execution	Critical	No	No	1
			CVE-2025-33061	Information Disclosure	Important	No	No	3
			CVE-2025-33059	Information Disclosure	Important	No	No	3
			CVE-2025-33065	Information Disclosure	Important	No	No	3

			CVE-2025-32712	Elevation of Privilege	Important	No	No	2
			CVE-2025-33053	Remote Code Execution	Important	No	Yes	0
			CVE-2025-33056	Denial of Service	Important	No	No	2
			CVE-2025-32724	Denial of Service	Important	No	No	3
			CVE-2025-33062	Information Disclosure	Important	No	No	3
			CVE-2025-32718	Elevation of Privilege	Important	No	No	3
			CVE-2025-24069	Information Disclosure	Important	No	No	2
			CVE-2025-24068	Information Disclosure	Important	No	No	2
			CVE-2025-29828	Remote Code Execution	Critical	No	No	2
			CVE-2025-33068	Denial of Service	Important	No	No	3
			CVE-2025-33052	Information Disclosure	Important	No	No	3
			CVE-2025-33067	Elevation of Privilege	Important	No	No	2
			CVE-2025-24065	Information Disclosure	Important	No	No	2
			CVE-2025-32725	Denial of Service	Important	No	No	2
			CVE-2025-32713	Elevation of Privilege	Important	No	No	1
			CVE-2025-33050	Denial of Service	Important	No	No	2
			CVE-2025-32721	Elevation of Privilege	Important	No	No	3
			CVE-2025-33064	Remote Code Execution	Important	No	No	3
			CVE-2025-33073	Elevation of Privilege	Important	Yes	No	2
			CVE-2025-33070	Elevation of Privilege	Critical	No	No	1

			CVE-2025-33066	Remote Code Execution	Important	No	No	3
			CVE-2025-33055	Information Disclosure	Important	No	No	3
			CVE-2025-32716	Elevation of Privilege	Important	No	No	3
			CVE-2025-33057	Denial of Service	Important	No	No	2
			CVE-2025-33063	Information Disclosure	Important	No	No	3
5060531	高危	June 10, 2025—KB5060531 (OS Build 17763.7434) - Microsoft Support for Win 10 Ent LTSC 2019,Win 10 IoT Ent LTSC 2019,Windows 10 IoT Core LTSC,Windows Server 2019	CVE-2025-33060	Information Disclosure	Important	No	No	3
			CVE-2025-32722	Information Disclosure	Important	No	No	2
			CVE-2025-32714	Elevation of Privilege	Important	No	No	1
			CVE-2025-33075	Elevation of Privilege	Important	No	No	2
			CVE-2025-33058	Information Disclosure	Important	No	No	2
			CVE-2025-32715	Information Disclosure	Important	No	No	2
			CVE-2025-32719	Information Disclosure	Important	No	No	3
			CVE-2025-47160	Security Feature Bypass	Important	No	No	2
			CVE-2025-32720	Information Disclosure	Important	No	No	3
			CVE-2025-3052	Security Feature Bypass	Important	No	No	2
			CVE-2025-33071	Remote Code Execution	Critical	No	No	1
			CVE-2025-33061	Information Disclosure	Important	No	No	3
			CVE-2025-33059	Information Disclosure	Important	No	No	3
			CVE-2025-33065	Information Disclosure	Important	No	No	3

			CVE-2025-32712	Elevation of Privilege	Important	No	No	2
			CVE-2025-33053	Remote Code Execution	Important	No	Yes	0
			CVE-2025-33056	Denial of Service	Important	No	No	2
			CVE-2025-32724	Denial of Service	Important	No	No	3
			CVE-2025-33062	Information Disclosure	Important	No	No	3
			CVE-2025-32718	Elevation of Privilege	Important	No	No	3
			CVE-2025-24069	Information Disclosure	Important	No	No	2
			CVE-2025-24068	Information Disclosure	Important	No	No	2
			CVE-2025-33068	Denial of Service	Important	No	No	3
			CVE-2025-33052	Information Disclosure	Important	No	No	3
			CVE-2025-33067	Elevation of Privilege	Important	No	No	2
			CVE-2025-24065	Information Disclosure	Important	No	No	2
			CVE-2025-32725	Denial of Service	Important	No	No	2
			CVE-2025-32713	Elevation of Privilege	Important	No	No	1
			CVE-2025-33050	Denial of Service	Important	No	No	2
			CVE-2025-32721	Elevation of Privilege	Important	No	No	3
			CVE-2025-33064	Remote Code Execution	Important	No	No	3
			CVE-2025-33073	Elevation of Privilege	Important	Yes	No	2
			CVE-2025-33070	Elevation of Privilege	Critical	No	No	1
			CVE-2025-33066	Remote Code Execution	Important	No	No	3

			CVE-2025-33055	Information Disclosure	Important	No	No	3
			CVE-2025-32716	Elevation of Privilege	Important	No	No	3
			CVE-2025-33057	Denial of Service	Important	No	No	2
			CVE-2025-33063	Information Disclosure	Important	No	No	3
5060999	高危	June 10, 2025—KB5060999 (OS Builds OS Builds 22621.5472 and 22631.5472) - Microsoft Support for Windows 11 Enterprise and Education, version 22H2,Windows 11 version 23H2, all editions	CVE-2025-33060	Information Disclosure	Important	No	No	3
			CVE-2025-32722	Information Disclosure	Important	No	No	2
			CVE-2025-32714	Elevation of Privilege	Important	No	No	1
			CVE-2025-33075	Elevation of Privilege	Important	No	No	2
			CVE-2025-33058	Information Disclosure	Important	No	No	2
			CVE-2025-32716	Elevation of Privilege	Important	No	No	3
			CVE-2025-32715	Information Disclosure	Important	No	No	2
			CVE-2025-47160	Security Feature Bypass	Important	No	No	2
			CVE-2025-32720	Information Disclosure	Important	No	No	3
			CVE-2025-3052	Security Feature Bypass	Important	No	No	2
			CVE-2025-33061	Information Disclosure	Important	No	No	3
			CVE-2025-33059	Information Disclosure	Important	No	No	3
			CVE-2025-33065	Information Disclosure	Important	No	No	3
			CVE-2025-32712	Elevation of Privilege	Important	No	No	2
			CVE-2025-33053	Remote Code Execution	Important	No	Yes	0

			CVE-2025-33056	Denial of Service	Important	No	No	2
			CVE-2025-32724	Denial of Service	Important	No	No	3
			CVE-2025-33062	Information Disclosure	Important	No	No	3
			CVE-2025-32718	Elevation of Privilege	Important	No	No	3
			CVE-2025-24069	Information Disclosure	Important	No	No	2
			CVE-2025-24068	Information Disclosure	Important	No	No	2
			CVE-2025-29828	Remote Code Execution	Critical	No	No	2
			CVE-2025-33052	Information Disclosure	Important	No	No	3
			CVE-2025-33067	Elevation of Privilege	Important	No	No	2
			CVE-2025-24065	Information Disclosure	Important	No	No	2
			CVE-2025-32713	Elevation of Privilege	Important	No	No	1
			CVE-2025-32721	Elevation of Privilege	Important	No	No	3
			CVE-2025-33064	Remote Code Execution	Important	No	No	3
			CVE-2025-33073	Elevation of Privilege	Important	Yes	No	2
			CVE-2025-33070	Elevation of Privilege	Critical	No	No	1
			CVE-2025-33066	Remote Code Execution	Important	No	No	3
			CVE-2025-33055	Information Disclosure	Important	No	No	3
			CVE-2025-32719	Information Disclosure	Important	No	No	3
			CVE-2025-33057	Denial of Service	Important	No	No	2
			CVE-2025-33063	Information Disclosure	Important	No	No	3

5060998	高危	June 10, 2025—KB5060998 (OS Build 10240.21034) - Microsoft Support for Windows 10	CVE-2025-33060	Information Disclosure	Important	No	No	3
			CVE-2025-32722	Information Disclosure	Important	No	No	2
			CVE-2025-32714	Elevation of Privilege	Important	No	No	1
			CVE-2025-33075	Elevation of Privilege	Important	No	No	2
			CVE-2025-33058	Information Disclosure	Important	No	No	2
			CVE-2025-32716	Elevation of Privilege	Important	No	No	3
			CVE-2025-32715	Information Disclosure	Important	No	No	2
			CVE-2025-47160	Security Feature Bypass	Important	No	No	2
			CVE-2025-32720	Information Disclosure	Important	No	No	3
			CVE-2025-3052	Security Feature Bypass	Important	No	No	2
			CVE-2025-33059	Information Disclosure	Important	No	No	3
			CVE-2025-33065	Information Disclosure	Important	No	No	3
			CVE-2025-32712	Elevation of Privilege	Important	No	No	2
			CVE-2025-33053	Remote Code Execution	Important	No	Yes	0
			CVE-2025-33056	Denial of Service	Important	No	No	2
			CVE-2025-32724	Denial of Service	Important	No	No	3
			CVE-2025-32718	Elevation of Privilege	Important	No	No	3
			CVE-2025-24069	Information Disclosure	Important	No	No	2
			CVE-2025-24068	Information Disclosure	Important	No	No	2

			CVE-2025-33067	Elevation of Privilege	Important	No	No	2
			CVE-2025-24065	Information Disclosure	Important	No	No	2
			CVE-2025-32713	Elevation of Privilege	Important	No	No	1
			CVE-2025-32721	Elevation of Privilege	Important	No	No	3
			CVE-2025-33064	Remote Code Execution	Important	No	No	3
			CVE-2025-33073	Elevation of Privilege	Important	Yes	No	2
			CVE-2025-33070	Elevation of Privilege	Critical	No	No	1
			CVE-2025-33066	Remote Code Execution	Important	No	No	3
			CVE-2025-33055	Information Disclosure	Important	No	No	3
			CVE-2025-32719	Information Disclosure	Important	No	No	3
			CVE-2025-33057	Denial of Service	Important	No	No	2
5061072	高危	June 10, 2025—KB5061072 (Security-only update) - Microsoft Support for Windows Server 2008 Premium Assurance	CVE-2025-32714	Elevation of Privilege	Important	No	No	1
			CVE-2025-33064	Remote Code Execution	Important	No	No	3
			CVE-2025-33075	Elevation of Privilege	Important	No	No	2
			CVE-2025-33073	Elevation of Privilege	Important	Yes	No	2
			CVE-2025-33066	Remote Code Execution	Important	No	No	3
			CVE-2025-33056	Denial of Service	Important	No	No	2
			CVE-2025-32712	Elevation of Privilege	Important	No	No	2
			CVE-2025-32716	Elevation of Privilege	Important	No	No	3
			CVE-2025-33057	Denial of Service	Important	No	No	2

			CVE-2025-32724	Denial of Service	Important	No	No	3
			CVE-2025-32713	Elevation of Privilege	Important	No	No	1
5061018	高危	June 10, 2025—KB5061018 (Monthly Rollup) - Microsoft Support for Windows Server 2012 R2 ESU	CVE-2025-33060	Information Disclosure	Important	No	No	3
			CVE-2025-32722	Information Disclosure	Important	No	No	2
			CVE-2025-32714	Elevation of Privilege	Important	No	No	1
			CVE-2025-33075	Elevation of Privilege	Important	No	No	2
			CVE-2025-32715	Information Disclosure	Important	No	No	2
			CVE-2025-32720	Information Disclosure	Important	No	No	3
			CVE-2025-47160	Security Feature Bypass	Important	No	No	2
			CVE-2025-3052	Security Feature Bypass	Important	No	No	2
			CVE-2025-33071	Remote Code Execution	Critical	No	No	1
			CVE-2025-32712	Elevation of Privilege	Important	No	No	2
			CVE-2025-33053	Remote Code Execution	Important	No	Yes	0
			CVE-2025-33056	Denial of Service	Important	No	No	2
			CVE-2025-32724	Denial of Service	Important	No	No	3
			CVE-2025-32718	Elevation of Privilege	Important	No	No	3
			CVE-2025-33068	Denial of Service	Important	No	No	3
			CVE-2025-32713	Elevation of Privilege	Important	No	No	1
			CVE-2025-33064	Remote Code Execution	Important	No	No	3

			CVE-2025-33073	Elevation of Privilege	Important	Yes	No	2
			CVE-2025-33070	Elevation of Privilege	Critical	No	No	1
			CVE-2025-33066	Remote Code Execution	Important	No	No	3
			CVE-2025-32716	Elevation of Privilege	Important	No	No	3
			CVE-2025-33057	Denial of Service	Important	No	No	2
5061026	高危	June 10, 2025—KB5061026 (Monthly Rollup) - Microsoft Support for Windows Server 2008 Premium Assurance	CVE-2025-32714	Elevation of Privilege	Important	No	No	1
			CVE-2025-33064	Remote Code Execution	Important	No	No	3
			CVE-2025-33075	Elevation of Privilege	Important	No	No	2
			CVE-2025-33073	Elevation of Privilege	Important	Yes	No	2
			CVE-2025-32716	Elevation of Privilege	Important	No	No	3
			CVE-2025-33066	Remote Code Execution	Important	No	No	3
			CVE-2025-33056	Denial of Service	Important	No	No	2
			CVE-2025-32712	Elevation of Privilege	Important	No	No	2
			CVE-2025-33053	Remote Code Execution	Important	No	Yes	0
			CVE-2025-33057	Denial of Service	Important	No	No	2
			CVE-2025-32724	Denial of Service	Important	No	No	3
			CVE-2025-32713	Elevation of Privilege	Important	No	No	1
5060533	高危	June 10, 2025—KB5060533 (OS Builds 19044.596	CVE-2025-33060	Information Disclosure	Important	No	No	3
			CVE-2025-32722	Information Disclosure	Important	No	No	2
			CVE-2025-32714	Elevation of Privilege	Important	No	No	1

		5 and 19045.5965) - Microsoft Support for Windows 10 Enterprise LTSC 2021,Windows 10 IoT Enterprise LTSC 2021,Windows 10, version 22H2, all editions	CVE-2025-33075	Elevation of Privilege	Important	No	No	2
			CVE-2025-33058	Information Disclosure	Important	No	No	2
			CVE-2025-32715	Information Disclosure	Important	No	No	2
			CVE-2025-32719	Information Disclosure	Important	No	No	3
			CVE-2025-47160	Security Feature Bypass	Important	No	No	2
			CVE-2025-32720	Information Disclosure	Important	No	No	3
			CVE-2025-3052	Security Feature Bypass	Important	No	No	2
			CVE-2025-33061	Information Disclosure	Important	No	No	3
			CVE-2025-33059	Information Disclosure	Important	No	No	3
			CVE-2025-33065	Information Disclosure	Important	No	No	3
			CVE-2025-32712	Elevation of Privilege	Important	No	No	2
			CVE-2025-33053	Remote Code Execution	Important	No	Yes	0
			CVE-2025-33056	Denial of Service	Important	No	No	2
			CVE-2025-32724	Denial of Service	Important	No	No	3
			CVE-2025-33062	Information Disclosure	Important	No	No	3
			CVE-2025-32718	Elevation of Privilege	Important	No	No	3
			CVE-2025-24069	Information Disclosure	Important	No	No	2
			CVE-2025-24068	Information Disclosure	Important	No	No	2
			CVE-2025-33052	Information Disclosure	Important	No	No	3

			CVE-2025-33067	Elevation of Privilege	Important	No	No	2
			CVE-2025-24065	Information Disclosure	Important	No	No	2
			CVE-2025-32713	Elevation of Privilege	Important	No	No	1
			CVE-2025-32721	Elevation of Privilege	Important	No	No	3
			CVE-2025-33064	Remote Code Execution	Important	No	No	3
			CVE-2025-33073	Elevation of Privilege	Important	Yes	No	2
			CVE-2025-33070	Elevation of Privilege	Critical	No	No	1
			CVE-2025-33066	Remote Code Execution	Important	No	No	3
			CVE-2025-33055	Information Disclosure	Important	No	No	3
			CVE-2025-32716	Elevation of Privilege	Important	No	No	3
			CVE-2025-33057	Denial of Service	Important	No	No	2
			CVE-2025-33063	Information Disclosure	Important	No	No	3
5061078	高危	June 10, 2025—KB5061078 (Monthly Rollup) - Microsoft Support for Windows Server 2008 R2 Premium Assurance	CVE-2025-32714	Elevation of Privilege	Important	No	No	1
			CVE-2025-33064	Remote Code Execution	Important	No	No	3
			CVE-2025-33075	Elevation of Privilege	Important	No	No	2
			CVE-2025-33073	Elevation of Privilege	Important	Yes	No	2
			CVE-2025-33070	Elevation of Privilege	Critical	No	No	1
			CVE-2025-32716	Elevation of Privilege	Important	No	No	3
			CVE-2025-33066	Remote Code Execution	Important	No	No	3
			CVE-2025-33056	Denial of Service	Important	No	No	2

			CVE-2025-32715	Information Disclosure	Important	No	No	2
			CVE-2025-33053	Remote Code Execution	Important	No	Yes	0
			CVE-2025-32712	Elevation of Privilege	Important	No	No	2
			CVE-2025-33057	Denial of Service	Important	No	No	2
			CVE-2025-32724	Denial of Service	Important	No	No	3
			CVE-2025-32713	Elevation of Privilege	Important	No	No	1
5061036	高危	June 10, 2025—KB5061036 (Security-only update) - Microsoft Support for Windows Server 2008 R2 Premium Assurance	CVE-2025-32714	Elevation of Privilege	Important	No	No	1
			CVE-2025-33064	Remote Code Execution	Important	No	No	3
			CVE-2025-33075	Elevation of Privilege	Important	No	No	2
			CVE-2025-33073	Elevation of Privilege	Important	Yes	No	2
			CVE-2025-33070	Elevation of Privilege	Critical	No	No	1
			CVE-2025-32715	Information Disclosure	Important	No	No	2
			CVE-2025-33066	Remote Code Execution	Important	No	No	3
			CVE-2025-33056	Denial of Service	Important	No	No	2
			CVE-2025-32712	Elevation of Privilege	Important	No	No	2
			CVE-2025-32716	Elevation of Privilege	Important	No	No	3
			CVE-2025-33057	Denial of Service	Important	No	No	2
			CVE-2025-32724	Denial of Service	Important	No	No	3
			CVE-2025-32713	Elevation of Privilege	Important	No	No	1
5061010	高危	June 10, 2025—	CVE-2025-33060	Information Disclosure	Important	No	No	3

		KB5061010 (OS Build 14393.8148) - Microsoft Support for Windows 10, version 1607, all editions, Windows Server 2016, all editions	CVE-2025-32722	Information Disclosure	Important	No	No	2
			CVE-2025-32714	Elevation of Privilege	Important	No	No	1
			CVE-2025-33075	Elevation of Privilege	Important	No	No	2
			CVE-2025-33058	Information Disclosure	Important	No	No	2
			CVE-2025-32716	Elevation of Privilege	Important	No	No	3
			CVE-2025-32715	Information Disclosure	Important	No	No	2
			CVE-2025-47160	Security Feature Bypass	Important	No	No	2
			CVE-2025-32720	Information Disclosure	Important	No	No	3
			CVE-2025-3052	Security Feature Bypass	Important	No	No	2
			CVE-2025-33071	Remote Code Execution	Critical	No	No	1
			CVE-2025-33061	Information Disclosure	Important	No	No	3
			CVE-2025-33059	Information Disclosure	Important	No	No	3
			CVE-2025-33065	Information Disclosure	Important	No	No	3
			CVE-2025-32712	Elevation of Privilege	Important	No	No	2
			CVE-2025-33053	Remote Code Execution	Important	No	Yes	0
			CVE-2025-33056	Denial of Service	Important	No	No	2
			CVE-2025-32724	Denial of Service	Important	No	No	3
			CVE-2025-33062	Information Disclosure	Important	No	No	3
			CVE-2025-32718	Elevation of Privilege	Important	No	No	3

			CVE-2025-24069	Information Disclosure	Important	No	No	2
			CVE-2025-24068	Information Disclosure	Important	No	No	2
			CVE-2025-33068	Denial of Service	Important	No	No	3
			CVE-2025-33067	Elevation of Privilege	Important	No	No	2
			CVE-2025-24065	Information Disclosure	Important	No	No	2
			CVE-2025-32725	Denial of Service	Important	No	No	2
			CVE-2025-32713	Elevation of Privilege	Important	No	No	1
			CVE-2025-33050	Denial of Service	Important	No	No	2
			CVE-2025-32721	Elevation of Privilege	Important	No	No	3
			CVE-2025-33064	Remote Code Execution	Important	No	No	3
			CVE-2025-33073	Elevation of Privilege	Important	Yes	No	2
			CVE-2025-33070	Elevation of Privilege	Critical	No	No	1
			CVE-2025-33066	Remote Code Execution	Important	No	No	3
			CVE-2025-33055	Information Disclosure	Important	No	No	3
			CVE-2025-32719	Information Disclosure	Important	No	No	3
			CVE-2025-33057	Denial of Service	Important	No	No	2
5060842	高危	June 10, 2025—KB5060842 (OS Build 26100.4349) - Microsoft Support	CVE-2025-33060	Information Disclosure	Important	No	No	3
			CVE-2025-32722	Information Disclosure	Important	No	No	2
			CVE-2025-32714	Elevation of Privilege	Important	No	No	1
			CVE-2025-33075	Elevation of Privilege	Important	No	No	2

		for Windows 11 version 24H2, all editions	CVE-2025-33058	Information Disclosure	Important	No	No	2
			CVE-2025-32715	Information Disclosure	Important	No	No	2
			CVE-2025-32720	Information Disclosure	Important	No	No	3
			CVE-2025-47160	Security Feature Bypass	Important	No	No	2
			CVE-2025-3052	Security Feature Bypass	Important	No	No	2
			CVE-2025-33071	Remote Code Execution	Critical	No	No	1
			CVE-2025-33061	Information Disclosure	Important	No	No	3
			CVE-2025-33059	Information Disclosure	Important	No	No	3
			CVE-2025-33065	Information Disclosure	Important	No	No	3
			CVE-2025-32712	Elevation of Privilege	Important	No	No	2
			CVE-2025-33053	Remote Code Execution	Important	No	Yes	0
			CVE-2025-33056	Denial of Service	Important	No	No	2
			CVE-2025-32724	Denial of Service	Important	No	No	3
			CVE-2025-33062	Information Disclosure	Important	No	No	3
			CVE-2025-32718	Elevation of Privilege	Important	No	No	3
			CVE-2025-24069	Information Disclosure	Important	No	No	2
			CVE-2025-24068	Information Disclosure	Important	No	No	2
			CVE-2025-29828	Remote Code Execution	Critical	No	No	2
			CVE-2025-33068	Denial of Service	Important	No	No	3

			CVE-2025-33052	Information Disclosure	Important	No	No	3
			CVE-2025-33067	Elevation of Privilege	Important	No	No	2
			CVE-2025-24065	Information Disclosure	Important	No	No	2
			CVE-2025-32725	Denial of Service	Important	No	No	2
			CVE-2025-32713	Elevation of Privilege	Important	No	No	1
			CVE-2025-33050	Denial of Service	Important	No	No	2
			CVE-2025-32721	Elevation of Privilege	Important	No	No	3
			CVE-2025-33064	Remote Code Execution	Important	No	No	3
			CVE-2025-33069	Security Feature Bypass	Important	No	No	2
			CVE-2025-33073	Elevation of Privilege	Important	Yes	No	2
			CVE-2025-33070	Elevation of Privilege	Critical	No	No	1
			CVE-2025-33066	Remote Code Execution	Important	No	No	3
			CVE-2025-33055	Information Disclosure	Important	No	No	3
			CVE-2025-32719	Information Disclosure	Important	No	No	3
			CVE-2025-33057	Denial of Service	Important	No	No	2
			CVE-2025-33063	Information Disclosure	Important	No	No	3
5061059	高危	June 10, 2025—KB5061059 (Monthly Rollup) - Microsoft Support for	CVE-2025-32722	Information Disclosure	Important	No	No	2
			CVE-2025-32714	Elevation of Privilege	Important	No	No	1
			CVE-2025-33075	Elevation of Privilege	Important	No	No	2
			CVE-2025-32715	Information Disclosure	Important	No	No	2

		Windows Server 2012 ESU	CVE-2025-47160	Security Feature Bypass	Important	No	No	2
			CVE-2025-3052	Security Feature Bypass	Important	No	No	2
			CVE-2025-33071	Remote Code Execution	Critical	No	No	1
			CVE-2025-32712	Elevation of Privilege	Important	No	No	2
			CVE-2025-33053	Remote Code Execution	Important	No	Yes	0
			CVE-2025-33056	Denial of Service	Important	No	No	2
			CVE-2025-32724	Denial of Service	Important	No	No	3
			CVE-2025-32718	Elevation of Privilege	Important	No	No	3
			CVE-2025-32713	Elevation of Privilege	Important	No	No	1
			CVE-2025-33064	Remote Code Execution	Important	No	No	3
			CVE-2025-33073	Elevation of Privilege	Important	Yes	No	2
			CVE-2025-33070	Elevation of Privilege	Critical	No	No	1
			CVE-2025-33066	Remote Code Execution	Important	No	No	3
			CVE-2025-32716	Elevation of Privilege	Important	No	No	3
			CVE-2025-33057	Denial of Service	Important	No	No	2

本月微软发布的软件安全更新补丁共 9 个，详细列表如下：

KBID	奇安信集团级别	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
5002735	高危	Description of the security update for Excel 2016: June 10, 2025 (KB5002735) - Microsoft Support	CVE-2025-47165	Remote Code Execution	Important	No	No	3
5002732	高危	Description of the security update for SharePoint Enterprise Server 2016: June 10, 2025 (KB5002732) - Microsoft Support	CVE-2025-47168	Remote Code Execution	Important	No	No	2
			CVE-2025-47169	Remote Code Execution	Important	No	No	2
			CVE-2025-47172	Remote Code Execution	Critical	No	No	2
			CVE-2025-47166	Remote Code Execution	Important	No	No	2
			CVE-2025-47163	Remote Code Execution	Important	No	No	2
5002616	高危	Description of the security update for Office 2016: June 10, 2025 (KB5002616) - Microsoft Support	CVE-2025-47167	Remote Code Execution	Critical	No	No	1

5002710	高危	Description of the security update for Word 2016: June 10, 2025 (KB5002710) - Microsoft Support	CVE-2025-47168	Remote Code Execution	Important	No	No	2
			CVE-2025-47169	Remote Code Execution	Important	No	No	2
5002683	高危	Description of the security update for Outlook 2016: June 10, 2025 (KB5002683) - Microsoft Support	CVE-2025-47171	Remote Code Execution	Important	No	No	3
5002730	高危	Description of the security update for Office 2016: June 10, 2025 (KB5002730) - Microsoft Support	CVE-2025-47162	Remote Code Execution	Critical	No	No	1
			CVE-2025-47164	Remote Code Execution	Critical	No	No	1
			CVE-2025-47173	Remote Code Execution	Important	No	No	3
			CVE-2025-47953	Remote Code Execution	Critical	No	No	2
5002689	高危	Description of the security update for PowerPoint 2016: June 10, 2025 (KB5002689) - Microsoft Support	CVE-2025-47175	Remote Code Execution	Important	No	No	2
5002731	高危	Description of the	CVE-2025-47168	Remote Code Execution	Important	No	No	2

		security update for SharePoint Enterprise Server 2016 Language Pack: June 10, 2025 (KB5002731) - Microsoft Support	CVE-2025-47169	Remote Code Execution	Important	No	No	2
5060996	高危	KB5060996: Cumulative security update for Internet Explorer: June 10, 2025 - Microsoft Support	CVE-2025-33053	Remote Code Execution	Important	No	Yes	0

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