奇安信集团 2024 年 08 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 08 月 14 日

目 录

文档信息

文档名称	奇安信集团 2024 年 08 月补丁库更新通告		
文档编号	Qi An Xin Group-MSPatch-2024-0801		
发布日期	2024-08-14	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:2024.08.14.1,V10版本:2024.08.14.1000)已发布，本次更新推送了20个微软安全补丁，修复了60个安全漏洞，其中6个微软官方评级为“严重(Critical)”，54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	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
5041782	CVE-2024-38198	Elevation of Privilege	Important	No	No	Exploitation More Likely
5041828						
5041823						
5041585						
5041838						
5041578						
5041847						
5041851						
5041160						
5041850						
5041571						
5041592						
5041580						
5041773						
5041782	CVE-2024-38063	Remote Code Execution	Critical	No	No	Exploitation More Likely
5041828						
5041823						
5041585						
5041838						
5041578						
5041847						
5041851						
5041160						
5041850						
5041571						
5041592						
5041580						
5041773						

5041782	CVE-2024-38199	Remote Code Execution	Important	Yes	No	Exploitation Less Likely
5041828						
5041823						
5041585						
5041838						
5041578						
5041847						
5041851						
5041160						
5041850						
5041571						
5041592						
5041580						
5041773						
5041782	CVE-2024-38107	Elevation of Privilege	Important	No	Yes	Exploitation Detected
5041828						
5041585						
5041578						
5041851						
5041160						
5041571						
5041592						
5041580						
5041773						
5041782	CVE-2024-38144	Elevation of Privilege	Important	No	No	Exploitation More Likely
5041828						
5041823						
5041585						
5041838						
5041578						
5041847						
5041851						
5041160						
5041850						
5041571						
5041592						
5041580						
5041773						
5041782	CVE-2024-38125	Elevation of Privilege	Important	No	No	Exploitation More Likely
5041828						
5041823						

5041585						
5041838						
5041578						
5041847						
5041851						
5041160						
5041850						
5041571						
5041592						
5041580						
5041773						
5041782	CVE-2024-38141	Elevation of Privilege	Important	No	No	Exploitation More Likely
5041828						
5041585						
5041578						
5041851						
5041160						
5041571						
5041592						
5041580						
5041773						
5041782	CVE-2024-38196	Elevation of Privilege	Important	No	No	Exploitation More Likely
5041828						
5041823						
5041585						
5041838						
5041578						
5041847						
5041851						
5041160						
5041850						
5041571						
5041592						
5041580						
5041773						
5041782	CVE-2022-3775	Remote Code Execution	Critical	No	No	Exploitation Less Likely
5041828						
5041585						
5041578						
5041851						
5041160						

5041571						
5041592						
5041580						
5041773						
5041782	CVE-2024-38193	Elevation of Privilege	Important	No	Yes	Exploitation Detected
5041828						
5041823						
5041585						
5041838						
5041578						
5041847						
5041851						
5041160						
5041850						
5041571						
5041592						
5041580						
5041773						
5041782	CVE-2023-40547	Security Feature Bypass	Critical	No	No	Exploitation Less Likely
5041828						
5041585						
5041578						
5041851						
5041160						
5041571						
5041592						
5041580						
5041773						
5041782	CVE-2024-38106	Elevation of Privilege	Important	No	Yes	Exploitation Detected
5041585						
5041578						
5041160						
5041571						
5041592						
5041580						
5041773						
5041782	CVE-2024-38178	Remote Code Execution	Important	No	Yes	Exploitation Detected
5041828						
5041585						
5041770						
5041578						

5041160						
5041571						
5041592						
5041580						
5041773						
5041782	CVE-2024-38140	Remote Code Execution	Critical	No	No	Exploitation Less Likely
5041828						
5041823						
5041585						
5041838						
5041578						
5041847						
5041851						
5041160						
5041850						
5041571						
5041592						
5041580						
5041773						
5041585	CVE-2024-38150	Elevation of Privilege	Important	No	No	Exploitation More Likely
5041160						
5041571						
5041592						
5041580						
5041585	CVE-2024-21302	Elevation of Privilege	Important	Yes	No	Exploitation Less Likely
5041578						
5041160						
5041571						
5041592						
5041580						
5041773						
5041585	CVE-2024-38133	Elevation of Privilege	Important	No	No	Exploitation More Likely
5041578						
5041160						
5041571						
5041592						
5041580						
5041585	CVE-2024-38148	Denial of Service	Important	No	No	Exploitation More Likely
5041160						
5041571						
5041592						

5041585	CVE-2024-38147	Elevation of Privilege	Important	No	No	Exploitation More Likely
5041160						
5041571						
5041592						
5041580						
5002570	CVE-2024-38200	Spoofing	Important	Yes	No	Exploitation Less Likely
5002625						
5002561	CVE-2024-38189	Remote Code Execution	Important	No	Yes	Exploitation Detected
5041773	CVE-2024-38160	Remote Code Execution	Critical	No	No	Exploitation Less Likely
5041773	CVE-2024-38159	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 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
5041782	高危	August 13, 2024—KB5041782 (OS Build 10240.20751) - Microsoft Support for Windows 10	CVE-2024-38198	Elevation of Privilege	Important	No	No	1
			CVE-2024-38063	Remote Code Execution	Critical	No	No	1
			CVE-2024-38146	Denial of Service	Important	No	No	2
			CVE-2024-38145	Denial of Service	Important	No	No	2
			CVE-2024-38127	Elevation of Privilege	Important	No	No	2
			CVE-2024-38132	Denial of Service	Important	No	No	2
			CVE-2024-38116	Remote Code Execution	Important	No	No	2
			CVE-2024-29995	Elevation of Privilege	Important	No	No	2
			CVE-2024-38115	Remote Code Execution	Important	No	No	2
			CVE-2024-38118	Information Disclosure	Important	No	No	2
			CVE-2024-38199	Remote Code Execution	Important	Yes	No	2
			CVE-2024-38107	Elevation of Privilege	Important	No	Yes	0
			CVE-2024-38144	Elevation of Privilege	Important	No	No	1
			CVE-2024-38131	Remote Code Execution	Important	No	No	2
			CVE-2024-38126	Denial of Service	Important	No	No	2

			CVE-2024-38125	Elevation of Privilege	Important	No	No	1
			CVE-2024-38114	Remote Code Execution	Important	No	No	2
			CVE-2024-38142	Elevation of Privilege	Important	No	No	2
			CVE-2024-38141	Elevation of Privilege	Important	No	No	1
			CVE-2024-38196	Elevation of Privilege	Important	No	No	1
			CVE-2022-3775	Remote Code Execution	Critical	No	No	2
			CVE-2024-38151	Information Disclosure	Important	No	No	2
			CVE-2024-38152	Remote Code Execution	Important	No	No	2
			CVE-2024-38223	Elevation of Privilege	Important	No	No	2
			CVE-2024-38193	Elevation of Privilege	Important	No	Yes	0
			CVE-2024-38143	Elevation of Privilege	Important	No	No	2
			CVE-2024-38180	Security Feature Bypass	Important	No	No	2
			CVE-2022-2601			No	No	2
			CVE-2023-40547	Security Feature Bypass	Critical	No	No	2
			CVE-2024-38106	Elevation of Privilege	Important	No	Yes	0
			CVE-2024-38122	Information Disclosure	Important	No	No	2
			CVE-2024-38117	Elevation of Privilege	Important	No	No	2
			CVE-2024-38153	Elevation of Privilege	Important	No	No	2
			CVE-2024-38178	Remote Code Execution	Important	No	Yes	0
			CVE-2024-38130	Remote Code Execution	Important	No	No	2

			CVE-2024-38140	Remote Code Execution	Critical	No	No	2
			CVE-2024-38134	Elevation of Privilege	Important	No	No	2
5041828	高危	August 13, 2024—KB5041828 (Monthly Rollup) - Microsoft Support for Windows Server 2012 R2 ESU	CVE-2024-38198	Elevation of Privilege	Important	No	No	1
			CVE-2024-38063	Remote Code Execution	Critical	No	No	1
			CVE-2024-38146	Denial of Service	Important	No	No	2
			CVE-2024-38145	Denial of Service	Important	No	No	2
			CVE-2024-38127	Elevation of Privilege	Important	No	No	2
			CVE-2024-38132	Denial of Service	Important	No	No	2
			CVE-2024-38116	Remote Code Execution	Important	No	No	2
			CVE-2024-38121	Remote Code Execution	Important	No	No	2
			CVE-2024-29995	Elevation of Privilege	Important	No	No	2
			CVE-2024-38120	Remote Code Execution	Important	No	No	2
			CVE-2024-38115	Remote Code Execution	Important	No	No	2
			CVE-2024-38118	Information Disclosure	Important	No	No	2
			CVE-2024-38199	Remote Code Execution	Important	Yes	No	2
			CVE-2024-38107	Elevation of Privilege	Important	No	Yes	0
			CVE-2024-38144	Elevation of Privilege	Important	No	No	1
			CVE-2024-38131	Remote Code Execution	Important	No	No	2
			CVE-2024-38126	Denial of Service	Important	No	No	2
			CVE-2024-38125	Elevation of Privilege	Important	No	No	1

			CVE-2024-38114	Remote Code Execution	Important	No	No	2
			CVE-2024-38214	Information Disclosure	Important	No	No	2
			CVE-2024-38128	Remote Code Execution	Important	No	No	2
			CVE-2024-38141	Elevation of Privilege	Important	No	No	1
			CVE-2024-37968	Spoofing	Important	No	No	2
			CVE-2024-38196	Elevation of Privilege	Important	No	No	1
			CVE-2022-3775	Remote Code Execution	Critical	No	No	2
			CVE-2024-38151	Information Disclosure	Important	No	No	2
			CVE-2024-38152	Remote Code Execution	Important	No	No	2
			CVE-2024-38223	Elevation of Privilege	Important	No	No	2
			CVE-2024-38193	Elevation of Privilege	Important	No	Yes	0
			CVE-2024-38180	Security Feature Bypass	Important	No	No	2
			CVE-2022-2601			No	No	2
			CVE-2023-40547	Security Feature Bypass	Critical	No	No	2
			CVE-2024-38122	Information Disclosure	Important	No	No	2
			CVE-2024-38117	Elevation of Privilege	Important	No	No	2
			CVE-2024-38153	Elevation of Privilege	Important	No	No	2
			CVE-2024-38130	Remote Code Execution	Important	No	No	2
			CVE-2024-38178	Remote Code Execution	Important	No	Yes	0
			CVE-2024-38154	Remote Code Execution	Important	No	No	2

			CVE-2024-38140	Remote Code Execution	Critical	No	No	2
			CVE-2024-38134	Elevation of Privilege	Important	No	No	2
5041823	高危	August 13, 2024—KB5041823 (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-2024-38198	Elevation of Privilege	Important	No	No	1
			CVE-2024-38063	Remote Code Execution	Critical	No	No	1
			CVE-2024-38127	Elevation of Privilege	Important	No	No	2
			CVE-2024-38116	Remote Code Execution	Important	No	No	2
			CVE-2024-38121	Remote Code Execution	Important	No	No	2
			CVE-2024-29995	Elevation of Privilege	Important	No	No	2
			CVE-2024-38120	Remote Code Execution	Important	No	No	2
			CVE-2024-38115	Remote Code Execution	Important	No	No	2
			CVE-2024-38118	Information Disclosure	Important	No	No	2
			CVE-2024-38199	Remote Code Execution	Important	Yes	No	2
			CVE-2024-38144	Elevation of Privilege	Important	No	No	1
			CVE-2024-38131	Remote Code Execution	Important	No	No	2
			CVE-2024-38114	Remote Code Execution	Important	No	No	2
			CVE-2024-38125	Elevation of Privilege	Important	No	No	1
			CVE-2024-38214	Information Disclosure	Important	No	No	2
			CVE-2024-38128	Remote Code Execution	Important	No	No	2
			CVE-2024-38196	Elevation of Privilege	Important	No	No	1
			CVE-2024-37968	Spoofing	Important	No	No	2
			CVE-2024-38151	Information Disclosure	Important	No	No	2

			CVE-2024-38152	Remote Code Execution	Important	No	No	2
			CVE-2024-38193	Elevation of Privilege	Important	No	Yes	0
			CVE-2024-38180	Security Feature Bypass	Important	No	No	2
			CVE-2024-38122	Information Disclosure	Important	No	No	2
			CVE-2024-38117	Elevation of Privilege	Important	No	No	2
			CVE-2024-38153	Elevation of Privilege	Important	No	No	2
			CVE-2024-38130	Remote Code Execution	Important	No	No	2
			CVE-2024-38154	Remote Code Execution	Important	No	No	2
			CVE-2024-38140	Remote Code Execution	Critical	No	No	2
			CVE-2024-38134	Elevation of Privilege	Important	No	No	2
5041585	高危	August 13, 2024—KB5041585 (OS Builds 22621.4037 and 22631.4037) - Microsoft Support for Windows 11 version 22H2, all editions,Windows 11 version 23H2, all editions	CVE-2024-38198	Elevation of Privilege	Important	No	No	1
			CVE-2024-38063	Remote Code Execution	Critical	No	No	1
			CVE-2024-38146	Denial of Service	Important	No	No	2
			CVE-2024-38215	Elevation of Privilege	Important	No	No	2
			CVE-2024-38145	Denial of Service	Important	No	No	2
			CVE-2024-38127	Elevation of Privilege	Important	No	No	2
			CVE-2024-38155	Information Disclosure	Important	No	No	2
			CVE-2024-38132	Denial of Service	Important	No	No	2
			CVE-2024-38116	Remote Code Execution	Important	No	No	2
			CVE-2024-38137	Elevation of Privilege	Important	No	No	2

			CVE-2024-38150	Elevation of Privilege	Important	No	No	1
			CVE-2024-38115	Remote Code Execution	Important	No	No	2
			CVE-2024-38118	Information Disclosure	Important	No	No	2
			CVE-2024-38199	Remote Code Execution	Important	Yes	No	2
			CVE-2024-21302	Elevation of Privilege	Important	Yes	No	2
			CVE-2024-38107	Elevation of Privilege	Important	No	Yes	0
			CVE-2024-38144	Elevation of Privilege	Important	No	No	1
			CVE-2024-38131	Remote Code Execution	Important	No	No	2
			CVE-2024-38126	Denial of Service	Important	No	No	2
			CVE-2024-38125	Elevation of Privilege	Important	No	No	1
			CVE-2024-38114	Remote Code Execution	Important	No	No	2
			CVE-2024-38142	Elevation of Privilege	Important	No	No	2
			CVE-2024-38141	Elevation of Privilege	Important	No	No	1
			CVE-2024-38196	Elevation of Privilege	Important	No	No	1
			CVE-2022-3775	Remote Code Execution	Critical	No	No	2
			CVE-2024-38151	Information Disclosure	Important	No	No	2
			CVE-2024-38133	Elevation of Privilege	Important	No	No	1
			CVE-2024-38152	Remote Code Execution	Important	No	No	2
			CVE-2024-38223	Elevation of Privilege	Important	No	No	2
			CVE-2024-38193	Elevation of Privilege	Important	No	Yes	0

			CVE-2024-38136	Elevation of Privilege	Important	No	No	2
			CVE-2024-38143	Elevation of Privilege	Important	No	No	2
			CVE-2024-38180	Security Feature Bypass	Important	No	No	2
			CVE-2022-2601			No	No	2
			CVE-2023-40547	Security Feature Bypass	Critical	No	No	2
			CVE-2024-38106	Elevation of Privilege	Important	No	Yes	0
			CVE-2024-38122	Information Disclosure	Important	No	No	2
			CVE-2024-38117	Elevation of Privilege	Important	No	No	2
			CVE-2024-38153	Elevation of Privilege	Important	No	No	2
			CVE-2024-38178	Remote Code Execution	Important	No	Yes	0
			CVE-2024-38130	Remote Code Execution	Important	No	No	2
			CVE-2024-38148	Denial of Service	Important	No	No	1
			CVE-2024-38140	Remote Code Execution	Critical	No	No	2
			CVE-2024-38147	Elevation of Privilege	Important	No	No	1
			CVE-2024-38135	Elevation of Privilege	Important	No	No	2
			CVE-2024-38134	Elevation of Privilege	Important	No	No	2
5041838	高危	August 13, 2024—KB5041838 (Monthly Rollup) - Microsoft Support for	CVE-2024-38198	Elevation of Privilege	Important	No	No	1
			CVE-2024-38063	Remote Code Execution	Critical	No	No	1
			CVE-2024-38127	Elevation of Privilege	Important	No	No	2
			CVE-2024-38116	Remote Code Execution	Important	No	No	2

		Windows Server 2008 R2 Enterprise ESU,Windows Server 2008 R2 Standard ESU,Windows Server 2008 R2 Datacenter ESU,Windows Embedded POSReady 7 ESU	CVE-2024-38121	Remote Code Execution	Important	No	No	2
			CVE-2024-29995	Elevation of Privilege	Important	No	No	2
			CVE-2024-38120	Remote Code Execution	Important	No	No	2
			CVE-2024-38115	Remote Code Execution	Important	No	No	2
			CVE-2024-38118	Information Disclosure	Important	No	No	2
			CVE-2024-38199	Remote Code Execution	Important	Yes	No	2
			CVE-2024-38144	Elevation of Privilege	Important	No	No	1
			CVE-2024-38131	Remote Code Execution	Important	No	No	2
			CVE-2024-38114	Remote Code Execution	Important	No	No	2
			CVE-2024-38125	Elevation of Privilege	Important	No	No	1
			CVE-2024-38214	Information Disclosure	Important	No	No	2
			CVE-2024-38128	Remote Code Execution	Important	No	No	2
			CVE-2024-38196	Elevation of Privilege	Important	No	No	1
			CVE-2024-37968	Spoofing	Important	No	No	2
			CVE-2024-38151	Information Disclosure	Important	No	No	2
			CVE-2024-38152	Remote Code Execution	Important	No	No	2
			CVE-2024-38193	Elevation of Privilege	Important	No	Yes	0
			CVE-2024-38180	Security Feature Bypass	Important	No	No	2
			CVE-2024-38122	Information Disclosure	Important	No	No	2
			CVE-2024-38117	Elevation of Privilege	Important	No	No	2

			CVE-2024-38153	Elevation of Privilege	Important	No	No	2
			CVE-2024-38130	Remote Code Execution	Important	No	No	2
			CVE-2024-38154	Remote Code Execution	Important	No	No	2
			CVE-2024-38140	Remote Code Execution	Critical	No	No	2
			CVE-2024-38134	Elevation of Privilege	Important	No	No	2
5041578	高危	August 13, 2024—KB5041578 (OS Build 17763.6189) - Microsoft Support for Win 10 Ent LTSC 2019,Win 10 IoT Ent LTSC 2019,Windows 10 IoT Core LTSC,Windows Server 2019	CVE-2024-38198	Elevation of Privilege	Important	No	No	1
			CVE-2024-38063	Remote Code Execution	Critical	No	No	1
			CVE-2024-38215	Elevation of Privilege	Important	No	No	2
			CVE-2024-38146	Denial of Service	Important	No	No	2
			CVE-2024-38145	Denial of Service	Important	No	No	2
			CVE-2024-38127	Elevation of Privilege	Important	No	No	2
			CVE-2024-38155	Information Disclosure	Important	No	No	2
			CVE-2024-38132	Denial of Service	Important	No	No	2
			CVE-2024-38116	Remote Code Execution	Important	No	No	2
			CVE-2024-38121	Remote Code Execution	Important	No	No	2
			CVE-2024-29995	Elevation of Privilege	Important	No	No	2
			CVE-2024-38120	Remote Code Execution	Important	No	No	2
			CVE-2024-38115	Remote Code Execution	Important	No	No	2
			CVE-2024-38118	Information Disclosure	Important	No	No	2
			CVE-2024-38199	Remote Code Execution	Important	Yes	No	2

			CVE-2024-21302	Elevation of Privilege	Important	Yes	No	2
			CVE-2024-38107	Elevation of Privilege	Important	No	Yes	0
			CVE-2024-38144	Elevation of Privilege	Important	No	No	1
			CVE-2024-38131	Remote Code Execution	Important	No	No	2
			CVE-2024-38126	Denial of Service	Important	No	No	2
			CVE-2024-38125	Elevation of Privilege	Important	No	No	1
			CVE-2024-38114	Remote Code Execution	Important	No	No	2
			CVE-2024-38214	Information Disclosure	Important	No	No	2
			CVE-2024-38142	Elevation of Privilege	Important	No	No	2
			CVE-2024-38128	Remote Code Execution	Important	No	No	2
			CVE-2024-38141	Elevation of Privilege	Important	No	No	1
			CVE-2024-37968	Spoofing	Important	No	No	2
			CVE-2024-38196	Elevation of Privilege	Important	No	No	1
			CVE-2022-3775	Remote Code Execution	Critical	No	No	2
			CVE-2024-38151	Information Disclosure	Important	No	No	2
			CVE-2024-38133	Elevation of Privilege	Important	No	No	1
			CVE-2024-38152	Remote Code Execution	Important	No	No	2
			CVE-2024-38223	Elevation of Privilege	Important	No	No	2
			CVE-2024-38193	Elevation of Privilege	Important	No	Yes	0
			CVE-2024-38136	Elevation of Privilege	Important	No	No	2

			CVE-2024-38180	Security Feature Bypass	Important	No	No	2
			CVE-2024-38143	Elevation of Privilege	Important	No	No	2
			CVE-2022-2601			No	No	2
			CVE-2023-40547	Security Feature Bypass	Critical	No	No	2
			CVE-2024-38106	Elevation of Privilege	Important	No	Yes	0
			CVE-2024-38122	Information Disclosure	Important	No	No	2
			CVE-2024-38117	Elevation of Privilege	Important	No	No	2
			CVE-2024-38153	Elevation of Privilege	Important	No	No	2
			CVE-2024-38130	Remote Code Execution	Important	No	No	2
			CVE-2024-38178	Remote Code Execution	Important	No	Yes	0
			CVE-2024-38154	Remote Code Execution	Important	No	No	2
			CVE-2024-38140	Remote Code Execution	Critical	No	No	2
			CVE-2024-38138	Remote Code Execution	Important	No	No	2
			CVE-2024-38134	Elevation of Privilege	Important	No	No	2
5041847	高危	August 13, 2024—KB5041847 (Security-only update) - Microsoft Support for Windows Server 2008	CVE-2024-38198	Elevation of Privilege	Important	No	No	1
			CVE-2024-38063	Remote Code Execution	Critical	No	No	1
			CVE-2024-38116	Remote Code Execution	Important	No	No	2
			CVE-2024-38121	Remote Code Execution	Important	No	No	2
			CVE-2024-29995	Elevation of Privilege	Important	No	No	2
			CVE-2024-38120	Remote Code Execution	Important	No	No	2

		Datacenter ESU,Windows Server 2008 Standard ESU,Windows Server 2008 Enterprise ESU	CVE-2024-38115	Remote Code Execution	Important	No	No	2
			CVE-2024-38118	Information Disclosure	Important	No	No	2
			CVE-2024-38199	Remote Code Execution	Important	Yes	No	2
			CVE-2024-38144	Elevation of Privilege	Important	No	No	1
			CVE-2024-38131	Remote Code Execution	Important	No	No	2
			CVE-2024-38114	Remote Code Execution	Important	No	No	2
			CVE-2024-38125	Elevation of Privilege	Important	No	No	1
			CVE-2024-38214	Information Disclosure	Important	No	No	2
			CVE-2024-38128	Remote Code Execution	Important	No	No	2
			CVE-2024-38196	Elevation of Privilege	Important	No	No	1
			CVE-2024-37968	Spoofing	Important	No	No	2
			CVE-2024-38151	Information Disclosure	Important	No	No	2
			CVE-2024-38152	Remote Code Execution	Important	No	No	2
			CVE-2024-38193	Elevation of Privilege	Important	No	Yes	0
			CVE-2024-38180	Security Feature Bypass	Important	No	No	2
			CVE-2024-38122	Information Disclosure	Important	No	No	2
			CVE-2024-38117	Elevation of Privilege	Important	No	No	2
			CVE-2024-38153	Elevation of Privilege	Important	No	No	2
			CVE-2024-38130	Remote Code Execution	Important	No	No	2
			CVE-2024-38154	Remote Code Execution	Important	No	No	2

			CVE-2024-38140	Remote Code Execution	Critical	No	No	2
			CVE-2024-38134	Elevation of Privilege	Important	No	No	2
5041851	高危	August 13, 2024—KB5041851 (Monthly Rollup) - Microsoft Support for Windows Server 2012 ESU	CVE-2024-38198	Elevation of Privilege	Important	No	No	1
			CVE-2024-38063	Remote Code Execution	Critical	No	No	1
			CVE-2024-38146	Denial of Service	Important	No	No	2
			CVE-2024-38145	Denial of Service	Important	No	No	2
			CVE-2024-38127	Elevation of Privilege	Important	No	No	2
			CVE-2024-38116	Remote Code Execution	Important	No	No	2
			CVE-2024-38121	Remote Code Execution	Important	No	No	2
			CVE-2024-29995	Elevation of Privilege	Important	No	No	2
			CVE-2024-38120	Remote Code Execution	Important	No	No	2
			CVE-2024-38115	Remote Code Execution	Important	No	No	2
			CVE-2024-38118	Information Disclosure	Important	No	No	2
			CVE-2024-38199	Remote Code Execution	Important	Yes	No	2
			CVE-2024-38107	Elevation of Privilege	Important	No	Yes	0
			CVE-2024-38144	Elevation of Privilege	Important	No	No	1
			CVE-2024-38131	Remote Code Execution	Important	No	No	2
			CVE-2024-38114	Remote Code Execution	Important	No	No	2
			CVE-2024-38125	Elevation of Privilege	Important	No	No	1
			CVE-2024-38214	Information Disclosure	Important	No	No	2

			CVE-2024-38128	Remote Code Execution	Important	No	No	2
			CVE-2024-38141	Elevation of Privilege	Important	No	No	1
			CVE-2024-37968	Spoofing	Important	No	No	2
			CVE-2024-38196	Elevation of Privilege	Important	No	No	1
			CVE-2022-3775	Remote Code Execution	Critical	No	No	2
			CVE-2024-38151	Information Disclosure	Important	No	No	2
			CVE-2024-38152	Remote Code Execution	Important	No	No	2
			CVE-2024-38193	Elevation of Privilege	Important	No	Yes	0
			CVE-2024-38180	Security Feature Bypass	Important	No	No	2
			CVE-2022-2601			No	No	2
			CVE-2023-40547	Security Feature Bypass	Critical	No	No	2
			CVE-2024-38122	Information Disclosure	Important	No	No	2
			CVE-2024-38117	Elevation of Privilege	Important	No	No	2
			CVE-2024-38153	Elevation of Privilege	Important	No	No	2
			CVE-2024-38130	Remote Code Execution	Important	No	No	2
			CVE-2024-38154	Remote Code Execution	Important	No	No	2
			CVE-2024-38140	Remote Code Execution	Critical	No	No	2
5041160	高危	August 13, 2024—KB5041160 (OS Build 20348.2655) -	CVE-2024-38198	Elevation of Privilege	Important	No	No	1
			CVE-2024-38063	Remote Code Execution	Critical	No	No	1
			CVE-2024-38215	Elevation of Privilege	Important	No	No	2

		Microsoft Support for Windows Server 2022	CVE-2024-38146	Denial of Service	Important	No	No	2
			CVE-2024-38145	Denial of Service	Important	No	No	2
			CVE-2024-38127	Elevation of Privilege	Important	No	No	2
			CVE-2024-38132	Denial of Service	Important	No	No	2
			CVE-2024-38116	Remote Code Execution	Important	No	No	2
			CVE-2024-38121	Remote Code Execution	Important	No	No	2
			CVE-2024-38137	Elevation of Privilege	Important	No	No	2
			CVE-2024-29995	Elevation of Privilege	Important	No	No	2
			CVE-2024-38120	Remote Code Execution	Important	No	No	2
			CVE-2024-38150	Elevation of Privilege	Important	No	No	1
			CVE-2024-38115	Remote Code Execution	Important	No	No	2
			CVE-2024-38118	Information Disclosure	Important	No	No	2
			CVE-2024-38199	Remote Code Execution	Important	Yes	No	2
			CVE-2024-21302	Elevation of Privilege	Important	Yes	No	2
			CVE-2024-38107	Elevation of Privilege	Important	No	Yes	0
			CVE-2024-38144	Elevation of Privilege	Important	No	No	1
			CVE-2024-38131	Remote Code Execution	Important	No	No	2
			CVE-2024-38126	Denial of Service	Important	No	No	2
			CVE-2024-38125	Elevation of Privilege	Important	No	No	1
			CVE-2024-38114	Remote Code Execution	Important	No	No	2

			CVE-2024-38214	Information Disclosure	Important	No	No	2
			CVE-2024-38142	Elevation of Privilege	Important	No	No	2
			CVE-2024-38128	Remote Code Execution	Important	No	No	2
			CVE-2024-38141	Elevation of Privilege	Important	No	No	1
			CVE-2024-37968	Spoofing	Important	No	No	2
			CVE-2024-38196	Elevation of Privilege	Important	No	No	1
			CVE-2022-3775	Remote Code Execution	Critical	No	No	2
			CVE-2024-38151	Information Disclosure	Important	No	No	2
			CVE-2024-38133	Elevation of Privilege	Important	No	No	1
			CVE-2024-38152	Remote Code Execution	Important	No	No	2
			CVE-2024-38223	Elevation of Privilege	Important	No	No	2
			CVE-2024-38193	Elevation of Privilege	Important	No	Yes	0
			CVE-2024-38136	Elevation of Privilege	Important	No	No	2
			CVE-2024-38180	Security Feature Bypass	Important	No	No	2
			CVE-2024-38143	Elevation of Privilege	Important	No	No	2
			CVE-2022-2601			No	No	2
			CVE-2023-40547	Security Feature Bypass	Critical	No	No	2
			CVE-2024-38106	Elevation of Privilege	Important	No	Yes	0
			CVE-2024-38122	Information Disclosure	Important	No	No	2
			CVE-2024-38117	Elevation of Privilege	Important	No	No	2

			CVE-2024-38153	Elevation of Privilege	Important	No	No	2
			CVE-2024-38130	Remote Code Execution	Important	No	No	2
			CVE-2024-38178	Remote Code Execution	Important	No	Yes	0
			CVE-2024-38154	Remote Code Execution	Important	No	No	2
			CVE-2024-38148	Denial of Service	Important	No	No	1
			CVE-2024-38140	Remote Code Execution	Critical	No	No	2
			CVE-2024-38147	Elevation of Privilege	Important	No	No	1
			CVE-2024-38138	Remote Code Execution	Important	No	No	2
			CVE-2024-38134	Elevation of Privilege	Important	No	No	2
5041850	高危	August 13, 2024—KB5041850 (Monthly Rollup) - Microsoft Support for Windows Server 2008 Datacenter ESU,Windows Server 2008 Standard ESU,Windows Server 2008 Enterprise ESU	CVE-2024-38198	Elevation of Privilege	Important	No	No	1
			CVE-2024-38063	Remote Code Execution	Critical	No	No	1
			CVE-2024-38116	Remote Code Execution	Important	No	No	2
			CVE-2024-38121	Remote Code Execution	Important	No	No	2
			CVE-2024-29995	Elevation of Privilege	Important	No	No	2
			CVE-2024-38120	Remote Code Execution	Important	No	No	2
			CVE-2024-38115	Remote Code Execution	Important	No	No	2
			CVE-2024-38118	Information Disclosure	Important	No	No	2
			CVE-2024-38199	Remote Code Execution	Important	Yes	No	2
			CVE-2024-38144	Elevation of Privilege	Important	No	No	1
			CVE-2024-38131	Remote Code Execution	Important	No	No	2

			CVE-2024-38114	Remote Code Execution	Important	No	No	2
			CVE-2024-38125	Elevation of Privilege	Important	No	No	1
			CVE-2024-38214	Information Disclosure	Important	No	No	2
			CVE-2024-38128	Remote Code Execution	Important	No	No	2
			CVE-2024-38196	Elevation of Privilege	Important	No	No	1
			CVE-2024-37968	Spoofing	Important	No	No	2
			CVE-2024-38151	Information Disclosure	Important	No	No	2
			CVE-2024-38152	Remote Code Execution	Important	No	No	2
			CVE-2024-38193	Elevation of Privilege	Important	No	Yes	0
			CVE-2024-38180	Security Feature Bypass	Important	No	No	2
			CVE-2024-38122	Information Disclosure	Important	No	No	2
			CVE-2024-38117	Elevation of Privilege	Important	No	No	2
			CVE-2024-38153	Elevation of Privilege	Important	No	No	2
			CVE-2024-38130	Remote Code Execution	Important	No	No	2
			CVE-2024-38154	Remote Code Execution	Important	No	No	2
			CVE-2024-38140	Remote Code Execution	Critical	No	No	2
			CVE-2024-38134	Elevation of Privilege	Important	No	No	2
5041571	高危	August 13, 2024—KB5041571 (OS Build 26100.1457) -	CVE-2024-38198	Elevation of Privilege	Important	No	No	1
			CVE-2024-38063	Remote Code Execution	Critical	No	No	1
			CVE-2024-38215	Elevation of Privilege	Important	No	No	2

		Microsoft Support for Windows 11 version 24H2, all editions	CVE-2024-38146	Denial of Service	Important	No	No	2
			CVE-2024-38145	Denial of Service	Important	No	No	2
			CVE-2024-38127	Elevation of Privilege	Important	No	No	2
			CVE-2024-38155	Information Disclosure	Important	No	No	2
			CVE-2024-38132	Denial of Service	Important	No	No	2
			CVE-2024-38116	Remote Code Execution	Important	No	No	2
			CVE-2024-38137	Elevation of Privilege	Important	No	No	2
			CVE-2024-38150	Elevation of Privilege	Important	No	No	1
			CVE-2024-38115	Remote Code Execution	Important	No	No	2
			CVE-2024-38118	Information Disclosure	Important	No	No	2
			CVE-2024-38199	Remote Code Execution	Important	Yes	No	2
			CVE-2024-21302	Elevation of Privilege	Important	Yes	No	2
			CVE-2024-38107	Elevation of Privilege	Important	No	Yes	0
			CVE-2024-38144	Elevation of Privilege	Important	No	No	1
			CVE-2024-38131	Remote Code Execution	Important	No	No	2
			CVE-2024-38126	Denial of Service	Important	No	No	2
			CVE-2024-38125	Elevation of Privilege	Important	No	No	1
			CVE-2024-38114	Remote Code Execution	Important	No	No	2
			CVE-2024-38142	Elevation of Privilege	Important	No	No	2
			CVE-2024-38141	Elevation of Privilege	Important	No	No	1

			CVE-2024-38196	Elevation of Privilege	Important	No	No	1
			CVE-2022-3775	Remote Code Execution	Critical	No	No	2
			CVE-2024-38151	Information Disclosure	Important	No	No	2
			CVE-2024-38133	Elevation of Privilege	Important	No	No	1
			CVE-2024-38152	Remote Code Execution	Important	No	No	2
			CVE-2024-38223	Elevation of Privilege	Important	No	No	2
			CVE-2024-38193	Elevation of Privilege	Important	No	Yes	0
			CVE-2024-38136	Elevation of Privilege	Important	No	No	2
			CVE-2024-38180	Security Feature Bypass	Important	No	No	2
			CVE-2024-38143	Elevation of Privilege	Important	No	No	2
			CVE-2022-2601			No	No	2
			CVE-2023-40547	Security Feature Bypass	Critical	No	No	2
			CVE-2024-38106	Elevation of Privilege	Important	No	Yes	0
			CVE-2024-38122	Information Disclosure	Important	No	No	2
			CVE-2024-38117	Elevation of Privilege	Important	No	No	2
			CVE-2024-38153	Elevation of Privilege	Important	No	No	2
			CVE-2024-38130	Remote Code Execution	Important	No	No	2
			CVE-2024-38178	Remote Code Execution	Important	No	Yes	0
			CVE-2024-38123	Information Disclosure	Important	No	No	2
			CVE-2024-38148	Denial of Service	Important	No	No	1

			CVE-2024-38140	Remote Code Execution	Critical	No	No	2
			CVE-2024-38147	Elevation of Privilege	Important	No	No	1
			CVE-2024-38135	Elevation of Privilege	Important	No	No	2
			CVE-2024-38134	Elevation of Privilege	Important	No	No	2
5041592	高危	August 13, 2024—KB5041592 (OS Build 22000.3147) - Microsoft Support for Windows 11 version 21H2, all editions	CVE-2024-38198	Elevation of Privilege	Important	No	No	1
			CVE-2024-38063	Remote Code Execution	Critical	No	No	1
			CVE-2024-38215	Elevation of Privilege	Important	No	No	2
			CVE-2024-38146	Denial of Service	Important	No	No	2
			CVE-2024-38145	Denial of Service	Important	No	No	2
			CVE-2024-38127	Elevation of Privilege	Important	No	No	2
			CVE-2024-38155	Information Disclosure	Important	No	No	2
			CVE-2024-38132	Denial of Service	Important	No	No	2
			CVE-2024-38116	Remote Code Execution	Important	No	No	2
			CVE-2024-38137	Elevation of Privilege	Important	No	No	2
			CVE-2024-38150	Elevation of Privilege	Important	No	No	1
			CVE-2024-38115	Remote Code Execution	Important	No	No	2
			CVE-2024-38118	Information Disclosure	Important	No	No	2
			CVE-2024-38199	Remote Code Execution	Important	Yes	No	2
			CVE-2024-21302	Elevation of Privilege	Important	Yes	No	2
			CVE-2024-38107	Elevation of Privilege	Important	No	Yes	0

			CVE-2024-38144	Elevation of Privilege	Important	No	No	1
			CVE-2024-38131	Remote Code Execution	Important	No	No	2
			CVE-2024-38126	Denial of Service	Important	No	No	2
			CVE-2024-38125	Elevation of Privilege	Important	No	No	1
			CVE-2024-38114	Remote Code Execution	Important	No	No	2
			CVE-2024-38142	Elevation of Privilege	Important	No	No	2
			CVE-2024-38141	Elevation of Privilege	Important	No	No	1
			CVE-2024-38196	Elevation of Privilege	Important	No	No	1
			CVE-2022-3775	Remote Code Execution	Critical	No	No	2
			CVE-2024-38151	Information Disclosure	Important	No	No	2
			CVE-2024-38133	Elevation of Privilege	Important	No	No	1
			CVE-2024-38152	Remote Code Execution	Important	No	No	2
			CVE-2024-38223	Elevation of Privilege	Important	No	No	2
			CVE-2024-38193	Elevation of Privilege	Important	No	Yes	0
			CVE-2024-38136	Elevation of Privilege	Important	No	No	2
			CVE-2024-38180	Security Feature Bypass	Important	No	No	2
			CVE-2024-38143	Elevation of Privilege	Important	No	No	2
			CVE-2022-2601			No	No	2
			CVE-2023-40547	Security Feature Bypass	Critical	No	No	2
			CVE-2024-38106	Elevation of Privilege	Important	No	Yes	0

			CVE-2024-38122	Information Disclosure	Important	No	No	2
			CVE-2024-38117	Elevation of Privilege	Important	No	No	2
			CVE-2024-38153	Elevation of Privilege	Important	No	No	2
			CVE-2024-38130	Remote Code Execution	Important	No	No	2
			CVE-2024-38178	Remote Code Execution	Important	No	Yes	0
			CVE-2024-38148	Denial of Service	Important	No	No	1
			CVE-2024-38140	Remote Code Execution	Critical	No	No	2
			CVE-2024-38147	Elevation of Privilege	Important	No	No	1
			CVE-2024-38134	Elevation of Privilege	Important	No	No	2
5041580	高危	August 13, 2024—KB5041580 (OS Builds 19044.4780 and 19045.4780) - Microsoft Support for Windows 10 Enterprise LTSC 2021,Windows 10 IoT Enterprise LTSC 2021,Windows 10, version	CVE-2024-38198	Elevation of Privilege	Important	No	No	1
			CVE-2024-38063	Remote Code Execution	Critical	No	No	1
			CVE-2024-38215	Elevation of Privilege	Important	No	No	2
			CVE-2024-38146	Denial of Service	Important	No	No	2
			CVE-2024-38145	Denial of Service	Important	No	No	2
			CVE-2024-38127	Elevation of Privilege	Important	No	No	2
			CVE-2024-38155	Information Disclosure	Important	No	No	2
			CVE-2024-38132	Denial of Service	Important	No	No	2
			CVE-2024-38116	Remote Code Execution	Important	No	No	2
			CVE-2024-38137	Elevation of Privilege	Important	No	No	2
			CVE-2024-29995	Elevation of Privilege	Important	No	No	2

		22H2, all editions	CVE-2024-38150	Elevation of Privilege	Important	No	No	1
			CVE-2024-38115	Remote Code Execution	Important	No	No	2
			CVE-2024-38118	Information Disclosure	Important	No	No	2
			CVE-2024-38199	Remote Code Execution	Important	Yes	No	2
			CVE-2024-21302	Elevation of Privilege	Important	Yes	No	2
			CVE-2024-38107	Elevation of Privilege	Important	No	Yes	0
			CVE-2024-38144	Elevation of Privilege	Important	No	No	1
			CVE-2024-38131	Remote Code Execution	Important	No	No	2
			CVE-2024-38126	Denial of Service	Important	No	No	2
			CVE-2024-38125	Elevation of Privilege	Important	No	No	1
			CVE-2024-38114	Remote Code Execution	Important	No	No	2
			CVE-2024-38142	Elevation of Privilege	Important	No	No	2
			CVE-2024-38141	Elevation of Privilege	Important	No	No	1
			CVE-2024-38196	Elevation of Privilege	Important	No	No	1
			CVE-2022-3775	Remote Code Execution	Critical	No	No	2
			CVE-2024-38151	Information Disclosure	Important	No	No	2
			CVE-2024-38133	Elevation of Privilege	Important	No	No	1
			CVE-2024-38152	Remote Code Execution	Important	No	No	2
			CVE-2024-38223	Elevation of Privilege	Important	No	No	2
			CVE-2024-38193	Elevation of Privilege	Important	No	Yes	0

			CVE-2024-38136	Elevation of Privilege	Important	No	No	2
			CVE-2024-38143	Elevation of Privilege	Important	No	No	2
			CVE-2024-38180	Security Feature Bypass	Important	No	No	2
			CVE-2022-2601			No	No	2
			CVE-2023-40547	Security Feature Bypass	Critical	No	No	2
			CVE-2024-38106	Elevation of Privilege	Important	No	Yes	0
			CVE-2024-38122	Information Disclosure	Important	No	No	2
			CVE-2024-38117	Elevation of Privilege	Important	No	No	2
			CVE-2024-38153	Elevation of Privilege	Important	No	No	2
			CVE-2024-38178	Remote Code Execution	Important	No	Yes	0
			CVE-2024-38130	Remote Code Execution	Important	No	No	2
			CVE-2024-38140	Remote Code Execution	Critical	No	No	2
			CVE-2024-38147	Elevation of Privilege	Important	No	No	1
			CVE-2024-38134	Elevation of Privilege	Important	No	No	2
5041773	高危	August 13, 2024—KB5041773 (OS Build 14393.7259) - Microsoft Support for Windows 10, version	CVE-2024-38198	Elevation of Privilege	Important	No	No	1
			CVE-2024-38063	Remote Code Execution	Critical	No	No	1
			CVE-2024-38146	Denial of Service	Important	No	No	2
			CVE-2024-38145	Denial of Service	Important	No	No	2
			CVE-2024-38127	Elevation of Privilege	Important	No	No	2
			CVE-2024-38132	Denial of Service	Important	No	No	2

		1607, all editions,Windows Server 2016, all editions	CVE-2024-38116	Remote Code Execution	Important	No	No	2
			CVE-2024-38121	Remote Code Execution	Important	No	No	2
			CVE-2024-29995	Elevation of Privilege	Important	No	No	2
			CVE-2024-38120	Remote Code Execution	Important	No	No	2
			CVE-2024-38115	Remote Code Execution	Important	No	No	2
			CVE-2024-38118	Information Disclosure	Important	No	No	2
			CVE-2024-38199	Remote Code Execution	Important	Yes	No	2
			CVE-2024-21302	Elevation of Privilege	Important	Yes	No	2
			CVE-2024-38107	Elevation of Privilege	Important	No	Yes	0
			CVE-2024-38144	Elevation of Privilege	Important	No	No	1
			CVE-2024-38131	Remote Code Execution	Important	No	No	2
			CVE-2024-38126	Denial of Service	Important	No	No	2
			CVE-2024-38125	Elevation of Privilege	Important	No	No	1
			CVE-2024-38114	Remote Code Execution	Important	No	No	2
			CVE-2024-38214	Information Disclosure	Important	No	No	2
			CVE-2024-38142	Elevation of Privilege	Important	No	No	2
			CVE-2024-38128	Remote Code Execution	Important	No	No	2
			CVE-2024-38141	Elevation of Privilege	Important	No	No	1
			CVE-2024-37968	Spoofing	Important	No	No	2
			CVE-2024-38196	Elevation of Privilege	Important	No	No	1
			CVE-2022-3775	Remote Code Execution	Critical	No	No	2

			CVE-2024-38151	Information Disclosure	Important	No	No	2
			CVE-2024-38152	Remote Code Execution	Important	No	No	2
			CVE-2024-38223	Elevation of Privilege	Important	No	No	2
			CVE-2024-38193	Elevation of Privilege	Important	No	Yes	0
			CVE-2024-38160	Remote Code Execution	Critical	No	No	2
			CVE-2024-38143	Elevation of Privilege	Important	No	No	2
			CVE-2024-38180	Security Feature Bypass	Important	No	No	2
			CVE-2022-2601			No	No	2
			CVE-2023-40547	Security Feature Bypass	Critical	No	No	2
			CVE-2024-38106	Elevation of Privilege	Important	No	Yes	0
			CVE-2024-38122	Information Disclosure	Important	No	No	2
			CVE-2024-38159	Remote Code Execution	Critical	No	No	2
			CVE-2024-38117	Elevation of Privilege	Important	No	No	2
			CVE-2024-38153	Elevation of Privilege	Important	No	No	2
			CVE-2024-38130	Remote Code Execution	Important	No	No	2
			CVE-2024-38178	Remote Code Execution	Important	No	Yes	0
			CVE-2024-38154	Remote Code Execution	Important	No	No	2
			CVE-2024-38140	Remote Code Execution	Critical	No	No	2
			CVE-2024-38138	Remote Code Execution	Important	No	No	2
			CVE-2024-38134	Elevation of Privilege	Important	No	No	2

本月微软发布的软件安全更新补丁共 6 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
5041770	高危	KB5041770: Cumulative security update for Internet Explorer: August 13, 2024 - Microsoft Support	CVE-2024-38178	Remote Code Execution	Important	No	Yes	0
5002570	高危	Description of the security update for Office 2016: August 13, 2024 (KB5002570) - Microsoft Support	CVE-2024-38200	Spoofing	Important	Yes	No	2

5002625	高危	Description of the security update for Office 2016: August 13, 2024 (KB5002625) - Microsoft Support	CVE-2024-38200	Spoofing	Important	Yes	No	2
5002561	高危	Description of the security update for Project 2016: August 13, 2024 (KB5002561) - Microsoft Support	CVE-2024-38189	Remote Code Execution	Important	No	Yes	0
5002586	高危	Description of the security update for PowerPoint 2016: August 13, 2024 (KB5002586) -	CVE-2024-38171	Remote Code Execution	Important	No	No	2

		Microsoft Support						
5002626	高危	Description of the security update for Outlook 2016: August 13, 2024 (KB5002626) - Microsoft Support	CVE-2024-38173	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