奇安信集团 2024 年 04 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 04 月 10 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 7

第 4 章 漏洞补丁详细列表 8

第 5 章 参考链接 57

文档信息

文档名称	奇安信集团 2024 年 04 月补丁库更新通告		
文档编号	Qi An Xin Group-MSPatch-2024-0401		
发布日期	2024-04-10	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:2024.04.10.1,V10版本:2024.04.10.1000)已发布，本次更新推送了27个微软安全补丁，修复了89个安全漏洞，均评级为“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 14 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
5036932	CVE-2024-26212	Denial of Service	Important	No	No	Exploitation More Likely
5036899						
5036950						
5036967						
5036969						
5036922						
5036896						
5036960						
5036909						
5036932	CVE-2024-26230	Elevation of Privilege	Important	No	No	Exploitation More Likely
5036899						
5036925						
5036893						
5036894						
5036950						
5036967						
5036969						
5036892						
5036922						
5036896						
5036960						
5036909						
5036932	CVE-2024-29056	Elevation of Privilege	Important	No	No	Exploitation More Likely
5036899						
5036950						
5036967						
5036969						
5036922						

5036896						
5036960						
5036909						
5036932	CVE-2024-26234	Spoofing	Important	Yes	Yes	Exploitation Detected
5036899						
5036925						
5036893						
5036894						
5036950						
5036967						
5036969						
5036892						
5036922						
5036896						
5036960						
5036909						
5036932	CVE-2024-26241	Elevation of Privilege	Important	No	No	Exploitation More Likely
5036899						
5036925						
5036893						
5036894						
5036950						
5036967						
5036969						
5036892						
5036922						
5036896						
5036960						
5036909						
5036932	CVE-2024-26158	Elevation of Privilege	Important	No	No	Exploitation More Likely
5036899						
5036925						
5036893						
5036894						
5036950						
5036967						
5036969						
5036892						
5036922						
5036896						
5036960						

5036909						
5036899	CVE-2024-26239	Elevation of Privilege	Important	No	No	Exploitation More Likely
5036925						
5036893						
5036894						
5036892						
5036896						
5036960						
5036909						
5036899	CVE-2024-28903	Security Feature Bypass	Important	No	No	Exploitation More Likely
5036925						
5036893						
5036894						
5036969						
5036892						
5036896						
5036960						
5036909						
5036899	CVE-2024-28921	Security Feature Bypass	Important	No	No	Exploitation More Likely
5036925						
5036893						
5036894						
5036969						
5036892						
5036896						
5036960						
5036909						
5036899	CVE-2024-26211	Elevation of Privilege	Important	No	No	Exploitation More Likely
5036925						
5036893						
5036894						
5036892						
5036896						
5036960						
5036909						
5036899	CVE-2024-26209	Information Disclosure	Important	No	No	Exploitation More Likely
5036925						
5036893						
5036894						
5036892						
5036896						

5036960 5036909						
5036893	CVE-2024-26256	Remote Code Execution	Important	No	No	Exploitation More Likely
5036893 5036894 5036892 5036896 5036909	CVE-2024-29988	Security Feature Bypass	Important	No	No	Exploitation More Likely
5036893 5036894 5036892 5036896 5036909	CVE-2024-26218	Elevation of Privilege	Important	No	No	Exploitation More Likely

第3章 已知问题和特殊调整

本月暂无已知问题和特殊调整。

第4章 漏洞补丁详细列表

本月微软发布的系统安全更新补丁共 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
5036932	高危	April 9, 2024—KB5036932 (Monthly Rollup) - Microsoft Support for Windows Server 2008 Datacenter ESU,Windows Server 2008 Standard ESU,Windows Server 2008 Enterprise ESU	CVE-2024-2201	Information Disclosure	Important	No	No	2
			CVE-2024-26232	Remote Code Execution	Important	No	No	2
			CVE-2024-26183	Denial of Service	Important	No	No	2
			CVE-2024-29050	Remote Code Execution	Important	No	No	2
			CVE-2024-26242	Elevation of Privilege	Important	No	No	2
			CVE-2024-26208	Remote Code Execution	Important	No	No	2
			CVE-2024-26215	Denial of Service	Important	No	No	2
			CVE-2024-26212	Denial of Service	Important	No	No	1
			CVE-2024-26252	Remote Code Execution	Important	No	No	2
			CVE-2024-28925	Security Feature Bypass	Important	No	No	2
			CVE-2024-26200	Remote Code Execution	Important	No	No	2
			CVE-2024-26230	Elevation of Privilege	Important	No	No	1
			CVE-2024-26248	Elevation of Privilege	Important	No	No	2
			CVE-2024-26229	Elevation of Privilege	Important	No	No	2

			CVE-2024-29056	Elevation of Privilege	Important	No	No	1
			CVE-2024-26234	Spoofing	Important	Yes	Yes	0
			CVE-2024-26228	Security Feature Bypass	Important	No	No	2
			CVE-2024-26179	Remote Code Execution	Important	No	No	2
			CVE-2024-26226	Information Disclosure	Important	No	No	2
			CVE-2024-26241	Elevation of Privilege	Important	No	No	1
			CVE-2024-26253	Remote Code Execution	Important	No	No	2
			CVE-2024-26205	Remote Code Execution	Important	No	No	2
			CVE-2024-26214	Remote Code Execution	Important	No	No	2
			CVE-2024-26210	Remote Code Execution	Important	No	No	2
			CVE-2024-26240	Security Feature Bypass	Important	No	No	2
			CVE-2024-26216	Elevation of Privilege	Important	No	No	2
			CVE-2024-26194	Security Feature Bypass	Important	No	No	2
			CVE-2024-29066	Remote Code Execution	Important	No	No	2
			CVE-2024-26244	Remote Code Execution	Important	No	No	2
			CVE-2024-26158	Elevation of Privilege	Important	No	No	1
			CVE-2024-20678	Remote Code Execution	Important	No	No	2
5036899	高危	April 9, 2024—KB5036899 (OS Build 14393.689	CVE-2024-2201	Information Disclosure	Important	No	No	2
			CVE-2024-28924	Security Feature Bypass	Important	No	No	2

		7) - Microsoft Support for Windows 10, version 1607, all editions, Windows Server 2016, all editions	CVE-2024-26232	Remote Code Execution	Important	No	No	2
			CVE-2024-20665	Security Feature Bypass	Important	No	No	2
			CVE-2024-26183	Denial of Service	Important	No	No	2
			CVE-2024-29050	Remote Code Execution	Important	No	No	2
			CVE-2024-26207	Information Disclosure	Important	No	No	2
			CVE-2024-26242	Elevation of Privilege	Important	No	No	2
			CVE-2024-28902	Information Disclosure	Important	No	No	2
			CVE-2024-26208	Remote Code Execution	Important	No	No	2
			CVE-2024-29064	Denial of Service	Important	No	No	2
			CVE-2024-26215	Denial of Service	Important	No	No	2
			CVE-2024-26212	Denial of Service	Important	No	No	1
			CVE-2024-26252	Remote Code Execution	Important	No	No	2
			CVE-2024-26222	Remote Code Execution	Important	No	No	2
			CVE-2024-20693	Elevation of Privilege	Important	No	No	2
			CVE-2024-28919	Security Feature Bypass	Important	No	No	2
			CVE-2024-28922	Security Feature Bypass	Important	No	No	2
			CVE-2024-26239	Elevation of Privilege	Important	No	No	1
			CVE-2024-28925	Security Feature Bypass	Important	No	No	2

			CVE-2024-28903	Security Feature Bypass	Important	No	No	1
			CVE-2024-26230	Elevation of Privilege	Important	No	No	1
			CVE-2024-28921	Security Feature Bypass	Important	No	No	1
			CVE-2024-26200	Remote Code Execution	Important	No	No	2
			CVE-2024-29061	Security Feature Bypass	Important	No	No	2
			CVE-2024-26248	Elevation of Privilege	Important	No	No	2
			CVE-2024-26233	Remote Code Execution	Important	No	No	2
			CVE-2024-26221	Remote Code Execution	Important	No	No	2
			CVE-2024-26168	Security Feature Bypass	Important	No	No	2
			CVE-2024-26227	Remote Code Execution	Important	No	No	2
			CVE-2024-26229	Elevation of Privilege	Important	No	No	2
			CVE-2024-21409	Remote Code Execution	Important	No	No	2
			CVE-2024-29056	Elevation of Privilege	Important	No	No	1
			CVE-2024-26234	Spoofing	Important	Yes	Yes	0
			CVE-2024-28896	Security Feature Bypass	Important	No	No	2
			CVE-2024-26228	Security Feature Bypass	Important	No	No	2
			CVE-2024-28900	Information Disclosure	Important	No	No	2
			CVE-2024-26179	Remote Code Execution	Important	No	No	2

			CVE-2024-26217	Information Disclosure	Important	No	No	2
			CVE-2024-29062	Security Feature Bypass	Important	No	No	2
			CVE-2024-26226	Information Disclosure	Important	No	No	2
			CVE-2024-26180	Security Feature Bypass	Important	No	No	2
			CVE-2024-28898	Security Feature Bypass	Important	No	No	2
			CVE-2024-26231	Remote Code Execution	Important	No	No	2
			CVE-2024-26195	Remote Code Execution	Important	No	No	2
			CVE-2024-28901	Information Disclosure	Important	No	No	2
			CVE-2024-26171	Security Feature Bypass	Important	No	No	2
			CVE-2024-26241	Elevation of Privilege	Important	No	No	1
			CVE-2024-26253	Remote Code Execution	Important	No	No	2
			CVE-2024-26211	Elevation of Privilege	Important	No	No	1
			CVE-2024-26214	Remote Code Execution	Important	No	No	2
			CVE-2024-26205	Remote Code Execution	Important	No	No	2
			CVE-2024-28923	Security Feature Bypass	Important	No	No	2
			CVE-2024-26175	Security Feature Bypass	Important	No	No	2
			CVE-2024-26210	Remote Code Execution	Important	No	No	2

			CVE-2024-26240	Security Feature Bypass	Important	No	No	2
			CVE-2024-28897	Security Feature Bypass	Important	No	No	2
			CVE-2024-26216	Elevation of Privilege	Important	No	No	2
			CVE-2024-26223	Remote Code Execution	Important	No	No	2
			CVE-2024-29066	Remote Code Execution	Important	No	No	2
			CVE-2024-26220	Information Disclosure	Important	No	No	2
			CVE-2024-20669	Security Feature Bypass	Important	No	No	2
			CVE-2024-26194	Security Feature Bypass	Important	No	No	2
			CVE-2024-26224	Remote Code Execution	Important	No	No	2
			CVE-2024-26244	Remote Code Execution	Important	No	No	2
			CVE-2024-26202	Remote Code Execution	Important	No	No	2
			CVE-2024-26158	Elevation of Privilege	Important	No	No	1
			CVE-2024-26250	Security Feature Bypass	Important	No	No	2
			CVE-2024-20678	Remote Code Execution	Important	No	No	2
			CVE-2024-26209	Information Disclosure	Important	No	No	1
			CVE-2024-26189	Security Feature Bypass	Important	No	No	2
5036925	高危	April 9, 2024—	CVE-2024-2201	Information Disclosure	Important	No	No	2

		KB5036925 (OS Build 10240.20596) - Microsoft Support for Windows 10	CVE-2024-28924	Security Feature Bypass	Important	No	No	2
			CVE-2024-26232	Remote Code Execution	Important	No	No	2
			CVE-2024-20665	Security Feature Bypass	Important	No	No	2
			CVE-2024-26183	Denial of Service	Important	No	No	2
			CVE-2024-29050	Remote Code Execution	Important	No	No	2
			CVE-2024-26207	Information Disclosure	Important	No	No	2
			CVE-2024-26242	Elevation of Privilege	Important	No	No	2
			CVE-2024-28902	Information Disclosure	Important	No	No	2
			CVE-2024-26208	Remote Code Execution	Important	No	No	2
			CVE-2024-29064	Denial of Service	Important	No	No	2
			CVE-2024-26252	Remote Code Execution	Important	No	No	2
			CVE-2024-20693	Elevation of Privilege	Important	No	No	2
			CVE-2024-28919	Security Feature Bypass	Important	No	No	2
			CVE-2024-28922	Security Feature Bypass	Important	No	No	2
			CVE-2024-26239	Elevation of Privilege	Important	No	No	1
			CVE-2024-28925	Security Feature Bypass	Important	No	No	2
			CVE-2024-28903	Security Feature Bypass	Important	No	No	1
			CVE-2024-26230	Elevation of Privilege	Important	No	No	1

			CVE-2024-28921	Security Feature Bypass	Important	No	No	1
			CVE-2024-26200	Remote Code Execution	Important	No	No	2
			CVE-2024-29061	Security Feature Bypass	Important	No	No	2
			CVE-2024-26248	Elevation of Privilege	Important	No	No	2
			CVE-2024-26168	Security Feature Bypass	Important	No	No	2
			CVE-2024-26229	Elevation of Privilege	Important	No	No	2
			CVE-2024-26234	Spoofing	Important	Yes	Yes	0
			CVE-2024-28896	Security Feature Bypass	Important	No	No	2
			CVE-2024-26228	Security Feature Bypass	Important	No	No	2
			CVE-2024-28900	Information Disclosure	Important	No	No	2
			CVE-2024-26179	Remote Code Execution	Important	No	No	2
			CVE-2024-26217	Information Disclosure	Important	No	No	2
			CVE-2024-29062	Security Feature Bypass	Important	No	No	2
			CVE-2024-26180	Security Feature Bypass	Important	No	No	2
			CVE-2024-28898	Security Feature Bypass	Important	No	No	2
			CVE-2024-26171	Security Feature Bypass	Important	No	No	2
			CVE-2024-28901	Information Disclosure	Important	No	No	2

			CVE-2024-26241	Elevation of Privilege	Important	No	No	1
			CVE-2024-26253	Remote Code Execution	Important	No	No	2
			CVE-2024-26211	Elevation of Privilege	Important	No	No	1
			CVE-2024-26214	Remote Code Execution	Important	No	No	2
			CVE-2024-26245	Elevation of Privilege	Important	No	No	2
			CVE-2024-28923	Security Feature Bypass	Important	No	No	2
			CVE-2024-26205	Remote Code Execution	Important	No	No	2
			CVE-2024-26175	Security Feature Bypass	Important	No	No	2
			CVE-2024-26210	Remote Code Execution	Important	No	No	2
			CVE-2024-26240	Security Feature Bypass	Important	No	No	2
			CVE-2024-28897	Security Feature Bypass	Important	No	No	2
			CVE-2024-26194	Security Feature Bypass	Important	No	No	2
			CVE-2024-26220	Information Disclosure	Important	No	No	2
			CVE-2024-20669	Security Feature Bypass	Important	No	No	2
			CVE-2024-26244	Remote Code Execution	Important	No	No	2
			CVE-2024-26158	Elevation of Privilege	Important	No	No	1
			CVE-2024-26250	Security Feature Bypass	Important	No	No	2

			CVE-2024-20678	Remote Code Execution	Important	No	No	2
			CVE-2024-26209	Information Disclosure	Important	No	No	1
			CVE-2024-26189	Security Feature Bypass	Important	No	No	2
5036893	高危	April 9, 2024—KB5036893 (OS Builds 22621.3447 and 22631.3447) - Microsoft Support for Windows 11 version 22H2, all editions, Windows 11 version 23H2, all editions	CVE-2024-26237	Elevation of Privilege	Important	No	No	2
			CVE-2024-23594	Security Feature Bypass	Important	No	No	2
			CVE-2024-2201	Information Disclosure	Important	No	No	2
			CVE-2024-28924	Security Feature Bypass	Important	No	No	2
			CVE-2024-26232	Remote Code Execution	Important	No	No	2
			CVE-2024-20665	Security Feature Bypass	Important	No	No	2
			CVE-2024-26183	Denial of Service	Important	No	No	2
			CVE-2024-29050	Remote Code Execution	Important	No	No	2
			CVE-2024-26207	Information Disclosure	Important	No	No	2
			CVE-2024-26242	Elevation of Privilege	Important	No	No	2
			CVE-2024-28902	Information Disclosure	Important	No	No	2
			CVE-2024-26208	Remote Code Execution	Important	No	No	2
			CVE-2024-29064	Denial of Service	Important	No	No	2
			CVE-2024-26252	Remote Code Execution	Important	No	No	2
			CVE-2024-26256	Remote Code Execution	Important	No	No	1
			CVE-2024-26209	Information Disclosure	Important	No	No	1

			CVE-2024-29988	Security Feature Bypass	Important	No	No	1
			CVE-2024-20693	Elevation of Privilege	Important	No	No	2
			CVE-2024-28919	Security Feature Bypass	Important	No	No	2
			CVE-2024-28922	Security Feature Bypass	Important	No	No	2
			CVE-2024-26239	Elevation of Privilege	Important	No	No	1
			CVE-2024-28925	Security Feature Bypass	Important	No	No	2
			CVE-2024-28903	Security Feature Bypass	Important	No	No	1
			CVE-2024-26230	Elevation of Privilege	Important	No	No	1
			CVE-2024-28921	Security Feature Bypass	Important	No	No	1
			CVE-2024-26200	Remote Code Execution	Important	No	No	2
			CVE-2024-29061	Security Feature Bypass	Important	No	No	2
			CVE-2024-26248	Elevation of Privilege	Important	No	No	2
			CVE-2024-26219	Denial of Service	Important	No	No	2
			CVE-2024-26168	Security Feature Bypass	Important	No	No	2
			CVE-2024-21447	Elevation of Privilege	Important	No	No	2
			CVE-2024-26229	Elevation of Privilege	Important	No	No	2
			CVE-2024-26234	Spoofing	Important	Yes	Yes	0

			CVE-2024-28896	Security Feature Bypass	Important	No	No	2
			CVE-2024-26228	Security Feature Bypass	Important	No	No	2
			CVE-2024-26254	Denial of Service	Important	No	No	2
			CVE-2024-28900	Information Disclosure	Important	No	No	2
			CVE-2024-26179	Remote Code Execution	Important	No	No	2
			CVE-2024-26217	Information Disclosure	Important	No	No	2
			CVE-2024-29062	Security Feature Bypass	Important	No	No	2
			CVE-2024-26180	Security Feature Bypass	Important	No	No	2
			CVE-2024-28898	Security Feature Bypass	Important	No	No	2
			CVE-2024-26171	Security Feature Bypass	Important	No	No	2
			CVE-2024-28901	Information Disclosure	Important	No	No	2
			CVE-2024-26241	Elevation of Privilege	Important	No	No	1
			CVE-2024-26253	Remote Code Execution	Important	No	No	2
			CVE-2024-26211	Elevation of Privilege	Important	No	No	1
			CVE-2024-26214	Remote Code Execution	Important	No	No	2
			CVE-2024-26205	Remote Code Execution	Important	No	No	2
			CVE-2024-28923	Security Feature Bypass	Important	No	No	2

			CVE-2024-26175	Security Feature Bypass	Important	No	No	2
			CVE-2024-26218	Elevation of Privilege	Important	No	No	1
			CVE-2024-26210	Remote Code Execution	Important	No	No	2
			CVE-2024-26240	Security Feature Bypass	Important	No	No	2
			CVE-2024-23593	Security Feature Bypass	Important	No	No	2
			CVE-2024-26194	Security Feature Bypass	Important	No	No	2
			CVE-2024-28897	Security Feature Bypass	Important	No	No	2
			CVE-2024-26220	Information Disclosure	Important	No	No	2
			CVE-2024-20669	Security Feature Bypass	Important	No	No	2
			CVE-2024-26244	Remote Code Execution	Important	No	No	2
			CVE-2024-26255	Information Disclosure	Important	No	No	2
			CVE-2024-28920	Security Feature Bypass	Important	No	No	2
			CVE-2024-26158	Elevation of Privilege	Important	No	No	1
			CVE-2024-26243	Elevation of Privilege	Important	No	No	2
			CVE-2024-26250	Security Feature Bypass	Important	No	No	2
			CVE-2024-20678	Remote Code Execution	Important	No	No	2
			CVE-2024-29052	Elevation of Privilege	Important	No	No	2

			CVE-2024-26189	Security Feature Bypass	Important	No	No	2
			CVE-2024-26172	Information Disclosure	Important	No	No	2
5036894	高危	April 9, 2024—KB5036894 (OS Build 22000.2899) - Microsoft Support for Windows 11 version 21H2, all editions	CVE-2024-26237	Elevation of Privilege	Important	No	No	2
			CVE-2024-23594	Security Feature Bypass	Important	No	No	2
			CVE-2024-2201	Information Disclosure	Important	No	No	2
			CVE-2024-28924	Security Feature Bypass	Important	No	No	2
			CVE-2024-26232	Remote Code Execution	Important	No	No	2
			CVE-2024-20665	Security Feature Bypass	Important	No	No	2
			CVE-2024-26183	Denial of Service	Important	No	No	2
			CVE-2024-29050	Remote Code Execution	Important	No	No	2
			CVE-2024-26207	Information Disclosure	Important	No	No	2
			CVE-2024-26242	Elevation of Privilege	Important	No	No	2
			CVE-2024-28902	Information Disclosure	Important	No	No	2
			CVE-2024-26208	Remote Code Execution	Important	No	No	2
			CVE-2024-29064	Denial of Service	Important	No	No	2
			CVE-2024-26252	Remote Code Execution	Important	No	No	2
			CVE-2024-26209	Information Disclosure	Important	No	No	1
			CVE-2024-29988	Security Feature Bypass	Important	No	No	1

			CVE-2024-20693	Elevation of Privilege	Important	No	No	2
			CVE-2024-28919	Security Feature Bypass	Important	No	No	2
			CVE-2024-28922	Security Feature Bypass	Important	No	No	2
			CVE-2024-26239	Elevation of Privilege	Important	No	No	1
			CVE-2024-28925	Security Feature Bypass	Important	No	No	2
			CVE-2024-28903	Security Feature Bypass	Important	No	No	1
			CVE-2024-26230	Elevation of Privilege	Important	No	No	1
			CVE-2024-28921	Security Feature Bypass	Important	No	No	1
			CVE-2024-26200	Remote Code Execution	Important	No	No	2
			CVE-2024-29061	Security Feature Bypass	Important	No	No	2
			CVE-2024-26248	Elevation of Privilege	Important	No	No	2
			CVE-2024-26219	Denial of Service	Important	No	No	2
			CVE-2024-26168	Security Feature Bypass	Important	No	No	2
			CVE-2024-21447	Elevation of Privilege	Important	No	No	2
			CVE-2024-26229	Elevation of Privilege	Important	No	No	2
			CVE-2024-26234	Spoofing	Important	Yes	Yes	0
			CVE-2024-28896	Security Feature Bypass	Important	No	No	2

			CVE-2024-26228	Security Feature Bypass	Important	No	No	2
			CVE-2024-26254	Denial of Service	Important	No	No	2
			CVE-2024-28900	Information Disclosure	Important	No	No	2
			CVE-2024-26179	Remote Code Execution	Important	No	No	2
			CVE-2024-26217	Information Disclosure	Important	No	No	2
			CVE-2024-29062	Security Feature Bypass	Important	No	No	2
			CVE-2024-26180	Security Feature Bypass	Important	No	No	2
			CVE-2024-28898	Security Feature Bypass	Important	No	No	2
			CVE-2024-26171	Security Feature Bypass	Important	No	No	2
			CVE-2024-28901	Information Disclosure	Important	No	No	2
			CVE-2024-26241	Elevation of Privilege	Important	No	No	1
			CVE-2024-26253	Remote Code Execution	Important	No	No	2
			CVE-2024-26211	Elevation of Privilege	Important	No	No	1
			CVE-2024-26214	Remote Code Execution	Important	No	No	2
			CVE-2024-26205	Remote Code Execution	Important	No	No	2
			CVE-2024-28923	Security Feature Bypass	Important	No	No	2
			CVE-2024-26175	Security Feature Bypass	Important	No	No	2

			CVE-2024-26218	Elevation of Privilege	Important	No	No	1
			CVE-2024-26210	Remote Code Execution	Important	No	No	2
			CVE-2024-26240	Security Feature Bypass	Important	No	No	2
			CVE-2024-23593	Security Feature Bypass	Important	No	No	2
			CVE-2024-26194	Security Feature Bypass	Important	No	No	2
			CVE-2024-28897	Security Feature Bypass	Important	No	No	2
			CVE-2024-26220	Information Disclosure	Important	No	No	2
			CVE-2024-20669	Security Feature Bypass	Important	No	No	2
			CVE-2024-26244	Remote Code Execution	Important	No	No	2
			CVE-2024-26255	Information Disclosure	Important	No	No	2
			CVE-2024-28920	Security Feature Bypass	Important	No	No	2
			CVE-2024-26158	Elevation of Privilege	Important	No	No	1
			CVE-2024-26243	Elevation of Privilege	Important	No	No	2
			CVE-2024-26250	Security Feature Bypass	Important	No	No	2
			CVE-2024-20678	Remote Code Execution	Important	No	No	2
			CVE-2024-29052	Elevation of Privilege	Important	No	No	2
			CVE-2024-26189	Security Feature Bypass	Important	No	No	2

			CVE-2024-26172	Information Disclosure	Important	No	No	2
5036950	高危	April 9, 2024—KB5036950 (Security-only update) - Microsoft Support for Windows Server 2008 Datacenter ESU,Windows Server 2008 Standard ESU,Windows Server 2008 Enterprise ESU	CVE-2024-2201	Information Disclosure	Important	No	No	2
			CVE-2024-26232	Remote Code Execution	Important	No	No	2
			CVE-2024-26183	Denial of Service	Important	No	No	2
			CVE-2024-29050	Remote Code Execution	Important	No	No	2
			CVE-2024-26242	Elevation of Privilege	Important	No	No	2
			CVE-2024-26208	Remote Code Execution	Important	No	No	2
			CVE-2024-26215	Denial of Service	Important	No	No	2
			CVE-2024-26212	Denial of Service	Important	No	No	1
			CVE-2024-26252	Remote Code Execution	Important	No	No	2
			CVE-2024-28925	Security Feature Bypass	Important	No	No	2
			CVE-2024-26200	Remote Code Execution	Important	No	No	2
			CVE-2024-26230	Elevation of Privilege	Important	No	No	1
			CVE-2024-26248	Elevation of Privilege	Important	No	No	2
			CVE-2024-26229	Elevation of Privilege	Important	No	No	2
			CVE-2024-29056	Elevation of Privilege	Important	No	No	1
			CVE-2024-26234	Spoofing	Important	Yes	Yes	0
			CVE-2024-26228	Security Feature Bypass	Important	No	No	2
			CVE-2024-26179	Remote Code Execution	Important	No	No	2
			CVE-2024-26226	Information Disclosure	Important	No	No	2

			CVE-2024-26241	Elevation of Privilege	Important	No	No	1
			CVE-2024-26253	Remote Code Execution	Important	No	No	2
			CVE-2024-26205	Remote Code Execution	Important	No	No	2
			CVE-2024-26214	Remote Code Execution	Important	No	No	2
			CVE-2024-26210	Remote Code Execution	Important	No	No	2
			CVE-2024-26240	Security Feature Bypass	Important	No	No	2
			CVE-2024-26216	Elevation of Privilege	Important	No	No	2
			CVE-2024-26194	Security Feature Bypass	Important	No	No	2
			CVE-2024-29066	Remote Code Execution	Important	No	No	2
			CVE-2024-26244	Remote Code Execution	Important	No	No	2
			CVE-2024-26158	Elevation of Privilege	Important	No	No	1
			CVE-2024-20678	Remote Code Execution	Important	No	No	2
5036967	高危	April 9, 2024—KB5036967 (Monthly Rollup) - Microsoft Support for Windows Server 2008 R2 Enterprise ESU,Windo	CVE-2024-2201	Information Disclosure	Important	No	No	2
			CVE-2024-26232	Remote Code Execution	Important	No	No	2
			CVE-2024-26183	Denial of Service	Important	No	No	2
			CVE-2024-29050	Remote Code Execution	Important	No	No	2
			CVE-2024-26242	Elevation of Privilege	Important	No	No	2
			CVE-2024-26208	Remote Code Execution	Important	No	No	2
			CVE-2024-26215	Denial of Service	Important	No	No	2

		ws Server 2008 R2 Standard ESU,Windows Server 2008 R2 Datacenter ESU,Windows Embedded POSReady 7 ESU	CVE-2024-26212	Denial of Service	Important	No	No	1
			CVE-2024-26252	Remote Code Execution	Important	No	No	2
			CVE-2024-28925	Security Feature Bypass	Important	No	No	2
			CVE-2024-26200	Remote Code Execution	Important	No	No	2
			CVE-2024-26230	Elevation of Privilege	Important	No	No	1
			CVE-2024-26248	Elevation of Privilege	Important	No	No	2
			CVE-2024-26229	Elevation of Privilege	Important	No	No	2
			CVE-2024-29056	Elevation of Privilege	Important	No	No	1
			CVE-2024-26234	Spoofing	Important	Yes	Yes	0
			CVE-2024-26228	Security Feature Bypass	Important	No	No	2
			CVE-2024-26179	Remote Code Execution	Important	No	No	2
			CVE-2024-26226	Information Disclosure	Important	No	No	2
			CVE-2024-26195	Remote Code Execution	Important	No	No	2
			CVE-2024-26241	Elevation of Privilege	Important	No	No	1
			CVE-2024-26253	Remote Code Execution	Important	No	No	2
			CVE-2024-26205	Remote Code Execution	Important	No	No	2
			CVE-2024-26214	Remote Code Execution	Important	No	No	2
			CVE-2024-26210	Remote Code Execution	Important	No	No	2
			CVE-2024-26240	Security Feature Bypass	Important	No	No	2

			CVE-2024-26216	Elevation of Privilege	Important	No	No	2
			CVE-2024-26194	Security Feature Bypass	Important	No	No	2
			CVE-2024-29066	Remote Code Execution	Important	No	No	2
			CVE-2024-26244	Remote Code Execution	Important	No	No	2
			CVE-2024-26158	Elevation of Privilege	Important	No	No	1
			CVE-2024-20678	Remote Code Execution	Important	No	No	2
5036969	高危	April 9, 2024—KB5036969 (Monthly Rollup) - Microsoft Support for Windows Server 2012 ESU	CVE-2024-20689	Security Feature Bypass	Important	No	No	2
			CVE-2024-2201	Information Disclosure	Important	No	No	2
			CVE-2024-20688	Security Feature Bypass	Important	No	No	2
			CVE-2024-28924	Security Feature Bypass	Important	No	No	2
			CVE-2024-26232	Remote Code Execution	Important	No	No	2
			CVE-2024-20665	Security Feature Bypass	Important	No	No	2
			CVE-2024-26183	Denial of Service	Important	No	No	2
			CVE-2024-29050	Remote Code Execution	Important	No	No	2
			CVE-2024-26242	Elevation of Privilege	Important	No	No	2
			CVE-2024-26208	Remote Code Execution	Important	No	No	2
			CVE-2024-26215	Denial of Service	Important	No	No	2
			CVE-2024-26212	Denial of Service	Important	No	No	1

			CVE-2024-26252	Remote Code Execution	Important	No	No	2
			CVE-2024-28919	Security Feature Bypass	Important	No	No	2
			CVE-2024-28922	Security Feature Bypass	Important	No	No	2
			CVE-2024-28925	Security Feature Bypass	Important	No	No	2
			CVE-2024-28903	Security Feature Bypass	Important	No	No	1
			CVE-2024-26230	Elevation of Privilege	Important	No	No	1
			CVE-2024-28921	Security Feature Bypass	Important	No	No	1
			CVE-2024-26200	Remote Code Execution	Important	No	No	2
			CVE-2024-29061	Security Feature Bypass	Important	No	No	2
			CVE-2024-26248	Elevation of Privilege	Important	No	No	2
			CVE-2024-26229	Elevation of Privilege	Important	No	No	2
			CVE-2024-29056	Elevation of Privilege	Important	No	No	1
			CVE-2024-26234	Spoofing	Important	Yes	Yes	0
			CVE-2024-28896	Security Feature Bypass	Important	No	No	2
			CVE-2024-26228	Security Feature Bypass	Important	No	No	2
			CVE-2024-26179	Remote Code Execution	Important	No	No	2
			CVE-2024-29062	Security Feature Bypass	Important	No	No	2

			CVE-2024-26226	Information Disclosure	Important	No	No	2
			CVE-2024-26180	Security Feature Bypass	Important	No	No	2
			CVE-2024-28898	Security Feature Bypass	Important	No	No	2
			CVE-2024-26195	Remote Code Execution	Important	No	No	2
			CVE-2024-26171	Security Feature Bypass	Important	No	No	2
			CVE-2024-26241	Elevation of Privilege	Important	No	No	1
			CVE-2024-26253	Remote Code Execution	Important	No	No	2
			CVE-2024-26205	Remote Code Execution	Important	No	No	2
			CVE-2024-26214	Remote Code Execution	Important	No	No	2
			CVE-2024-26175	Security Feature Bypass	Important	No	No	2
			CVE-2024-28923	Security Feature Bypass	Important	No	No	2
			CVE-2024-26210	Remote Code Execution	Important	No	No	2
			CVE-2024-26240	Security Feature Bypass	Important	No	No	2
			CVE-2024-28897	Security Feature Bypass	Important	No	No	2
			CVE-2024-26194	Security Feature Bypass	Important	No	No	2
			CVE-2024-26216	Elevation of Privilege	Important	No	No	2
			CVE-2024-29066	Remote Code Execution	Important	No	No	2

			CVE-2024-20669	Security Feature Bypass	Important	No	No	2
			CVE-2024-26244	Remote Code Execution	Important	No	No	2
			CVE-2024-26202	Remote Code Execution	Important	No	No	2
			CVE-2024-26158	Elevation of Privilege	Important	No	No	1
			CVE-2024-26250	Security Feature Bypass	Important	No	No	2
			CVE-2024-20678	Remote Code Execution	Important	No	No	2
			CVE-2024-26189	Security Feature Bypass	Important	No	No	2
5036892	高危	April 9, 2024—KB5036892 (OS Builds 19044.4291 and 19045.4291) - Microsoft Support for Windows 10 Enterprise and Education, version 21H2,Windows 10 IoT Enterprise, version 21H2,Wind	CVE-2024-26237	Elevation of Privilege	Important	No	No	2
			CVE-2024-23594	Security Feature Bypass	Important	No	No	2
			CVE-2024-2201	Information Disclosure	Important	No	No	2
			CVE-2024-28924	Security Feature Bypass	Important	No	No	2
			CVE-2024-26232	Remote Code Execution	Important	No	No	2
			CVE-2024-20665	Security Feature Bypass	Important	No	No	2
			CVE-2024-26183	Denial of Service	Important	No	No	2
			CVE-2024-29050	Remote Code Execution	Important	No	No	2
			CVE-2024-26207	Information Disclosure	Important	No	No	2
			CVE-2024-26242	Elevation of Privilege	Important	No	No	2
			CVE-2024-28902	Information Disclosure	Important	No	No	2

		ows 10 Enterprise Multi-Session, version 21H2,Windows 10, version 22H2, all editions, Windows 10 Enterprise LTSC 2021,Windows 10 IoT Enterprise LTSC 2021	CVE-2024-26208	Remote Code Execution	Important	No	No	2
			CVE-2024-29064	Denial of Service	Important	No	No	2
			CVE-2024-26252	Remote Code Execution	Important	No	No	2
			CVE-2024-26209	Information Disclosure	Important	No	No	1
			CVE-2024-29988	Security Feature Bypass	Important	No	No	1
			CVE-2024-20693	Elevation of Privilege	Important	No	No	2
			CVE-2024-28919	Security Feature Bypass	Important	No	No	2
			CVE-2024-28922	Security Feature Bypass	Important	No	No	2
			CVE-2024-26239	Elevation of Privilege	Important	No	No	1
			CVE-2024-28925	Security Feature Bypass	Important	No	No	2
			CVE-2024-28903	Security Feature Bypass	Important	No	No	1
			CVE-2024-26230	Elevation of Privilege	Important	No	No	1
			CVE-2024-28921	Security Feature Bypass	Important	No	No	1
			CVE-2024-26200	Remote Code Execution	Important	No	No	2
			CVE-2024-29061	Security Feature Bypass	Important	No	No	2
			CVE-2024-26248	Elevation of Privilege	Important	No	No	2
			CVE-2024-26219	Denial of Service	Important	No	No	2

			CVE-2024-26168	Security Feature Bypass	Important	No	No	2
			CVE-2024-21447	Elevation of Privilege	Important	No	No	2
			CVE-2024-26229	Elevation of Privilege	Important	No	No	2
			CVE-2024-26234	Spoofing	Important	Yes	Yes	0
			CVE-2024-28896	Security Feature Bypass	Important	No	No	2
			CVE-2024-26228	Security Feature Bypass	Important	No	No	2
			CVE-2024-26254	Denial of Service	Important	No	No	2
			CVE-2024-28900	Information Disclosure	Important	No	No	2
			CVE-2024-26179	Remote Code Execution	Important	No	No	2
			CVE-2024-26217	Information Disclosure	Important	No	No	2
			CVE-2024-29062	Security Feature Bypass	Important	No	No	2
			CVE-2024-26180	Security Feature Bypass	Important	No	No	2
			CVE-2024-28898	Security Feature Bypass	Important	No	No	2
			CVE-2024-26171	Security Feature Bypass	Important	No	No	2
			CVE-2024-28901	Information Disclosure	Important	No	No	2
			CVE-2024-26241	Elevation of Privilege	Important	No	No	1
			CVE-2024-26253	Remote Code Execution	Important	No	No	2
			CVE-2024-26211	Elevation of Privilege	Important	No	No	1

			CVE-2024-26214	Remote Code Execution	Important	No	No	2
			CVE-2024-26205	Remote Code Execution	Important	No	No	2
			CVE-2024-28923	Security Feature Bypass	Important	No	No	2
			CVE-2024-26175	Security Feature Bypass	Important	No	No	2
			CVE-2024-26218	Elevation of Privilege	Important	No	No	1
			CVE-2024-26210	Remote Code Execution	Important	No	No	2
			CVE-2024-26240	Security Feature Bypass	Important	No	No	2
			CVE-2024-23593	Security Feature Bypass	Important	No	No	2
			CVE-2024-26194	Security Feature Bypass	Important	No	No	2
			CVE-2024-28897	Security Feature Bypass	Important	No	No	2
			CVE-2024-26220	Information Disclosure	Important	No	No	2
			CVE-2024-20669	Security Feature Bypass	Important	No	No	2
			CVE-2024-26244	Remote Code Execution	Important	No	No	2
			CVE-2024-26255	Information Disclosure	Important	No	No	2
			CVE-2024-28920	Security Feature Bypass	Important	No	No	2
			CVE-2024-26158	Elevation of Privilege	Important	No	No	1
			CVE-2024-26243	Elevation of Privilege	Important	No	No	2

			CVE-2024-26250	Security Feature Bypass	Important	No	No	2
			CVE-2024-20678	Remote Code Execution	Important	No	No	2
			CVE-2024-29052	Elevation of Privilege	Important	No	No	2
			CVE-2024-26189	Security Feature Bypass	Important	No	No	2
			CVE-2024-26172	Information Disclosure	Important	No	No	2
5036922	高危	April 9, 2024—KB5036922 (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-2024-2201	Information Disclosure	Important	No	No	2
			CVE-2024-26232	Remote Code Execution	Important	No	No	2
			CVE-2024-26183	Denial of Service	Important	No	No	2
			CVE-2024-29050	Remote Code Execution	Important	No	No	2
			CVE-2024-26242	Elevation of Privilege	Important	No	No	2
			CVE-2024-26208	Remote Code Execution	Important	No	No	2
			CVE-2024-26215	Denial of Service	Important	No	No	2
			CVE-2024-26212	Denial of Service	Important	No	No	1
			CVE-2024-26252	Remote Code Execution	Important	No	No	2
			CVE-2024-28925	Security Feature Bypass	Important	No	No	2
			CVE-2024-26200	Remote Code Execution	Important	No	No	2
			CVE-2024-26230	Elevation of Privilege	Important	No	No	1
			CVE-2024-26248	Elevation of Privilege	Important	No	No	2
			CVE-2024-26229	Elevation of Privilege	Important	No	No	2

			CVE-2024-29056	Elevation of Privilege	Important	No	No	1
			CVE-2024-26234	Spoofing	Important	Yes	Yes	0
			CVE-2024-26228	Security Feature Bypass	Important	No	No	2
			CVE-2024-26179	Remote Code Execution	Important	No	No	2
			CVE-2024-26226	Information Disclosure	Important	No	No	2
			CVE-2024-26195	Remote Code Execution	Important	No	No	2
			CVE-2024-26241	Elevation of Privilege	Important	No	No	1
			CVE-2024-26253	Remote Code Execution	Important	No	No	2
			CVE-2024-26205	Remote Code Execution	Important	No	No	2
			CVE-2024-26214	Remote Code Execution	Important	No	No	2
			CVE-2024-26210	Remote Code Execution	Important	No	No	2
			CVE-2024-26240	Security Feature Bypass	Important	No	No	2
			CVE-2024-26216	Elevation of Privilege	Important	No	No	2
			CVE-2024-26194	Security Feature Bypass	Important	No	No	2
			CVE-2024-29066	Remote Code Execution	Important	No	No	2
			CVE-2024-26244	Remote Code Execution	Important	No	No	2
			CVE-2024-26158	Elevation of Privilege	Important	No	No	1
			CVE-2024-20678	Remote Code Execution	Important	No	No	2
5036896	高危	April 9, 2024—	CVE-2024-26237	Elevation of Privilege	Important	No	No	2

		KB5036896 (OS Build 17763.5696) - Microsoft Support for Win 10 Ent LTSC 2019,Win 10 IoT Ent LTSC 2019,Windows 10 IoT Core 2019 LTSC,Windows Server 2019	CVE-2024-2201	Information Disclosure	Important	No	No	2
			CVE-2024-26208	Remote Code Execution	Important	No	No	2
			CVE-2024-29064	Denial of Service	Important	No	No	2
			CVE-2024-20693	Elevation of Privilege	Important	No	No	2
			CVE-2024-26239	Elevation of Privilege	Important	No	No	1
			CVE-2024-26219	Denial of Service	Important	No	No	2
			CVE-2024-26230	Elevation of Privilege	Important	No	No	1
			CVE-2024-29061	Security Feature Bypass	Important	No	No	2
			CVE-2024-26227	Remote Code Execution	Important	No	No	2
			CVE-2024-26228	Security Feature Bypass	Important	No	No	2
			CVE-2024-28900	Information Disclosure	Important	No	No	2
			CVE-2024-26179	Remote Code Execution	Important	No	No	2
			CVE-2024-26180	Security Feature Bypass	Important	No	No	2
			CVE-2024-28898	Security Feature Bypass	Important	No	No	2
			CVE-2024-26195	Remote Code Execution	Important	No	No	2
			CVE-2024-26253	Remote Code Execution	Important	No	No	2
			CVE-2024-26211	Elevation of Privilege	Important	No	No	1
			CVE-2024-26214	Remote Code Execution	Important	No	No	2

			CVE-2024-26175	Security Feature Bypass	Important	No	No	2
			CVE-2024-26210	Remote Code Execution	Important	No	No	2
			CVE-2024-23593	Security Feature Bypass	Important	No	No	2
			CVE-2024-26220	Information Disclosure	Important	No	No	2
			CVE-2024-26202	Remote Code Execution	Important	No	No	2
			CVE-2024-26250	Security Feature Bypass	Important	No	No	2
			CVE-2024-28896	Security Feature Bypass	Important	No	No	2
			CVE-2024-26189	Security Feature Bypass	Important	No	No	2
			CVE-2024-28924	Security Feature Bypass	Important	No	No	2
			CVE-2024-29050	Remote Code Execution	Important	No	No	2
			CVE-2024-26207	Information Disclosure	Important	No	No	2
			CVE-2024-26252	Remote Code Execution	Important	No	No	2
			CVE-2024-26222	Remote Code Execution	Important	No	No	2
			CVE-2024-26200	Remote Code Execution	Important	No	No	2
			CVE-2024-26234	Spoofing	Important	Yes	Yes	0
			CVE-2024-26231	Remote Code Execution	Important	No	No	2
			CVE-2024-26241	Elevation of Privilege	Important	No	No	1
			CVE-2024-26216	Elevation of Privilege	Important	No	No	2

			CVE-2024-26223	Remote Code Execution	Important	No	No	2
			CVE-2024-26158	Elevation of Privilege	Important	No	No	1
			CVE-2024-20678	Remote Code Execution	Important	No	No	2
			CVE-2024-26232	Remote Code Execution	Important	No	No	2
			CVE-2024-20665	Security Feature Bypass	Important	No	No	2
			CVE-2024-26183	Denial of Service	Important	No	No	2
			CVE-2024-26242	Elevation of Privilege	Important	No	No	2
			CVE-2024-28902	Information Disclosure	Important	No	No	2
			CVE-2024-29988	Security Feature Bypass	Important	No	No	1
			CVE-2024-28922	Security Feature Bypass	Important	No	No	2
			CVE-2024-28921	Security Feature Bypass	Important	No	No	1
			CVE-2024-26168	Security Feature Bypass	Important	No	No	2
			CVE-2024-26221	Remote Code Execution	Important	No	No	2
			CVE-2024-29056	Elevation of Privilege	Important	No	No	1
			CVE-2024-26254	Denial of Service	Important	No	No	2
			CVE-2024-28901	Information Disclosure	Important	No	No	2
			CVE-2024-26205	Remote Code Execution	Important	No	No	2
			CVE-2024-28923	Security Feature Bypass	Important	No	No	2

			CVE-2024-26240	Security Feature Bypass	Important	No	No	2
			CVE-2024-28897	Security Feature Bypass	Important	No	No	2
			CVE-2024-29066	Remote Code Execution	Important	No	No	2
			CVE-2024-26209	Information Disclosure	Important	No	No	1
			CVE-2024-23594	Security Feature Bypass	Important	No	No	2
			CVE-2024-26215	Denial of Service	Important	No	No	2
			CVE-2024-26212	Denial of Service	Important	No	No	1
			CVE-2024-28919	Security Feature Bypass	Important	No	No	2
			CVE-2024-28925	Security Feature Bypass	Important	No	No	2
			CVE-2024-28903	Security Feature Bypass	Important	No	No	1
			CVE-2024-26248	Elevation of Privilege	Important	No	No	2
			CVE-2024-26233	Remote Code Execution	Important	No	No	2
			CVE-2024-26229	Elevation of Privilege	Important	No	No	2
			CVE-2024-26217	Information Disclosure	Important	No	No	2
			CVE-2024-26226	Information Disclosure	Important	No	No	2
			CVE-2024-29062	Security Feature Bypass	Important	No	No	2
			CVE-2024-26218	Elevation of Privilege	Important	No	No	1

			CVE-2024-26194	Security Feature Bypass	Important	No	No	2
			CVE-2024-26224	Remote Code Execution	Important	No	No	2
			CVE-2024-20669	Security Feature Bypass	Important	No	No	2
			CVE-2024-26244	Remote Code Execution	Important	No	No	2
			CVE-2024-26255	Information Disclosure	Important	No	No	2
			CVE-2024-28920	Security Feature Bypass	Important	No	No	2
			CVE-2024-26171	Security Feature Bypass	Important	No	No	2
			CVE-2024-26172	Information Disclosure	Important	No	No	2
5036960	高危	April 9, 2024—KB5036960 (Monthly Rollup) - Microsoft Support for Windows Server 2012 R2 ESU	CVE-2024-20689	Security Feature Bypass	Important	No	No	2
			CVE-2024-2201	Information Disclosure	Important	No	No	2
			CVE-2024-20688	Security Feature Bypass	Important	No	No	2
			CVE-2024-28924	Security Feature Bypass	Important	No	No	2
			CVE-2024-26232	Remote Code Execution	Important	No	No	2
			CVE-2024-20665	Security Feature Bypass	Important	No	No	2
			CVE-2024-26183	Denial of Service	Important	No	No	2
			CVE-2024-29050	Remote Code Execution	Important	No	No	2
			CVE-2024-26207	Information Disclosure	Important	No	No	2

			CVE-2024-26242	Elevation of Privilege	Important	No	No	2
			CVE-2024-28902	Information Disclosure	Important	No	No	2
			CVE-2024-26208	Remote Code Execution	Important	No	No	2
			CVE-2024-26215	Denial of Service	Important	No	No	2
			CVE-2024-26212	Denial of Service	Important	No	No	1
			CVE-2024-26252	Remote Code Execution	Important	No	No	2
			CVE-2024-28919	Security Feature Bypass	Important	No	No	2
			CVE-2024-28922	Security Feature Bypass	Important	No	No	2
			CVE-2024-26239	Elevation of Privilege	Important	No	No	1
			CVE-2024-28925	Security Feature Bypass	Important	No	No	2
			CVE-2024-28903	Security Feature Bypass	Important	No	No	1
			CVE-2024-26230	Elevation of Privilege	Important	No	No	1
			CVE-2024-28921	Security Feature Bypass	Important	No	No	1
			CVE-2024-26200	Remote Code Execution	Important	No	No	2
			CVE-2024-29061	Security Feature Bypass	Important	No	No	2
			CVE-2024-26248	Elevation of Privilege	Important	No	No	2
			CVE-2024-26168	Security Feature Bypass	Important	No	No	2

			CVE-2024-26229	Elevation of Privilege	Important	No	No	2
			CVE-2024-29056	Elevation of Privilege	Important	No	No	1
			CVE-2024-26234	Spoofing	Important	Yes	Yes	0
			CVE-2024-28896	Security Feature Bypass	Important	No	No	2
			CVE-2024-26228	Security Feature Bypass	Important	No	No	2
			CVE-2024-28900	Information Disclosure	Important	No	No	2
			CVE-2024-26179	Remote Code Execution	Important	No	No	2
			CVE-2024-26217	Information Disclosure	Important	No	No	2
			CVE-2024-26226	Information Disclosure	Important	No	No	2
			CVE-2024-29062	Security Feature Bypass	Important	No	No	2
			CVE-2024-26180	Security Feature Bypass	Important	No	No	2
			CVE-2024-28898	Security Feature Bypass	Important	No	No	2
			CVE-2024-26195	Remote Code Execution	Important	No	No	2
			CVE-2024-26171	Security Feature Bypass	Important	No	No	2
			CVE-2024-28901	Information Disclosure	Important	No	No	2
			CVE-2024-26241	Elevation of Privilege	Important	No	No	1
			CVE-2024-26253	Remote Code Execution	Important	No	No	2
			CVE-2024-26211	Elevation of Privilege	Important	No	No	1

			CVE-2024-26214	Remote Code Execution	Important	No	No	2
			CVE-2024-26205	Remote Code Execution	Important	No	No	2
			CVE-2024-28923	Security Feature Bypass	Important	No	No	2
			CVE-2024-26175	Security Feature Bypass	Important	No	No	2
			CVE-2024-26210	Remote Code Execution	Important	No	No	2
			CVE-2024-26240	Security Feature Bypass	Important	No	No	2
			CVE-2024-28897	Security Feature Bypass	Important	No	No	2
			CVE-2024-26194	Security Feature Bypass	Important	No	No	2
			CVE-2024-26216	Elevation of Privilege	Important	No	No	2
			CVE-2024-29066	Remote Code Execution	Important	No	No	2
			CVE-2024-20669	Security Feature Bypass	Important	No	No	2
			CVE-2024-26244	Remote Code Execution	Important	No	No	2
			CVE-2024-26202	Remote Code Execution	Important	No	No	2
			CVE-2024-26158	Elevation of Privilege	Important	No	No	1
			CVE-2024-26250	Security Feature Bypass	Important	No	No	2
			CVE-2024-20678	Remote Code Execution	Important	No	No	2
			CVE-2024-26209	Information Disclosure	Important	No	No	1

			CVE-2024-26189	Security Feature Bypass	Important	No	No	2
5036909	高危	April 9, 2024—KB5036909 (OS Build 20348.2402) - Microsoft Support for Windows Server 2022	CVE-2024-26237	Elevation of Privilege	Important	No	No	2
			CVE-2024-2201	Information Disclosure	Important	No	No	2
			CVE-2024-26208	Remote Code Execution	Important	No	No	2
			CVE-2024-29064	Denial of Service	Important	No	No	2
			CVE-2024-20693	Elevation of Privilege	Important	No	No	2
			CVE-2024-26239	Elevation of Privilege	Important	No	No	1
			CVE-2024-26219	Denial of Service	Important	No	No	2
			CVE-2024-26230	Elevation of Privilege	Important	No	No	1
			CVE-2024-29061	Security Feature Bypass	Important	No	No	2
			CVE-2024-21447	Elevation of Privilege	Important	No	No	2
			CVE-2024-26227	Remote Code Execution	Important	No	No	2
			CVE-2024-26228	Security Feature Bypass	Important	No	No	2
			CVE-2024-28900	Information Disclosure	Important	No	No	2
			CVE-2024-26179	Remote Code Execution	Important	No	No	2
			CVE-2024-26180	Security Feature Bypass	Important	No	No	2
			CVE-2024-28898	Security Feature Bypass	Important	No	No	2
			CVE-2024-26195	Remote Code Execution	Important	No	No	2

			CVE-2024-26253	Remote Code Execution	Important	No	No	2
			CVE-2024-26211	Elevation of Privilege	Important	No	No	1
			CVE-2024-26214	Remote Code Execution	Important	No	No	2
			CVE-2024-26175	Security Feature Bypass	Important	No	No	2
			CVE-2024-26210	Remote Code Execution	Important	No	No	2
			CVE-2024-23593	Security Feature Bypass	Important	No	No	2
			CVE-2024-26220	Information Disclosure	Important	No	No	2
			CVE-2024-26202	Remote Code Execution	Important	No	No	2
			CVE-2024-26243	Elevation of Privilege	Important	No	No	2
			CVE-2024-26250	Security Feature Bypass	Important	No	No	2
			CVE-2024-28896	Security Feature Bypass	Important	No	No	2
			CVE-2024-29052	Elevation of Privilege	Important	No	No	2
			CVE-2024-26189	Security Feature Bypass	Important	No	No	2
			CVE-2024-28924	Security Feature Bypass	Important	No	No	2
			CVE-2024-29050	Remote Code Execution	Important	No	No	2
			CVE-2024-26207	Information Disclosure	Important	No	No	2
			CVE-2024-26252	Remote Code Execution	Important	No	No	2
			CVE-2024-26222	Remote Code Execution	Important	No	No	2

			CVE-2024-26200	Remote Code Execution	Important	No	No	2
			CVE-2024-26234	Spoofing	Important	Yes	Yes	0
			CVE-2024-26231	Remote Code Execution	Important	No	No	2
			CVE-2024-26241	Elevation of Privilege	Important	No	No	1
			CVE-2024-26216	Elevation of Privilege	Important	No	No	2
			CVE-2024-26223	Remote Code Execution	Important	No	No	2
			CVE-2024-26158	Elevation of Privilege	Important	No	No	1
			CVE-2024-20678	Remote Code Execution	Important	No	No	2
			CVE-2024-26232	Remote Code Execution	Important	No	No	2
			CVE-2024-20665	Security Feature Bypass	Important	No	No	2
			CVE-2024-26183	Denial of Service	Important	No	No	2
			CVE-2024-26242	Elevation of Privilege	Important	No	No	2
			CVE-2024-28902	Information Disclosure	Important	No	No	2
			CVE-2024-29988	Security Feature Bypass	Important	No	No	1
			CVE-2024-28922	Security Feature Bypass	Important	No	No	2
			CVE-2024-28921	Security Feature Bypass	Important	No	No	1
			CVE-2024-26168	Security Feature Bypass	Important	No	No	2
			CVE-2024-26221	Remote Code Execution	Important	No	No	2
			CVE-2024-29056	Elevation of Privilege	Important	No	No	1

			CVE-2024-26254	Denial of Service	Important	No	No	2
			CVE-2024-28901	Information Disclosure	Important	No	No	2
			CVE-2024-26205	Remote Code Execution	Important	No	No	2
			CVE-2024-28923	Security Feature Bypass	Important	No	No	2
			CVE-2024-26240	Security Feature Bypass	Important	No	No	2
			CVE-2024-28897	Security Feature Bypass	Important	No	No	2
			CVE-2024-29066	Remote Code Execution	Important	No	No	2
			CVE-2024-26209	Information Disclosure	Important	No	No	1
			CVE-2024-23594	Security Feature Bypass	Important	No	No	2
			CVE-2024-26215	Denial of Service	Important	No	No	2
			CVE-2024-26212	Denial of Service	Important	No	No	1
			CVE-2024-28919	Security Feature Bypass	Important	No	No	2
			CVE-2024-28925	Security Feature Bypass	Important	No	No	2
			CVE-2024-28903	Security Feature Bypass	Important	No	No	1
			CVE-2024-26248	Elevation of Privilege	Important	No	No	2
			CVE-2024-26233	Remote Code Execution	Important	No	No	2
			CVE-2024-26229	Elevation of Privilege	Important	No	No	2

			CVE-2024-26217	Information Disclosure	Important	No	No	2
			CVE-2024-29062	Security Feature Bypass	Important	No	No	2
			CVE-2024-26226	Information Disclosure	Important	No	No	2
			CVE-2024-26218	Elevation of Privilege	Important	No	No	1
			CVE-2024-26194	Security Feature Bypass	Important	No	No	2
			CVE-2024-26224	Remote Code Execution	Important	No	No	2
			CVE-2024-20669	Security Feature Bypass	Important	No	No	2
			CVE-2024-26244	Remote Code Execution	Important	No	No	2
			CVE-2024-26255	Information Disclosure	Important	No	No	2
			CVE-2024-28920	Security Feature Bypass	Important	No	No	2
			CVE-2024-26171	Security Feature Bypass	Important	No	No	2
			CVE-2024-26172	Information Disclosure	Important	No	No	2

本月微软发布的软件安全更新补丁共 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
5036609	高危	April 9, 2024- KB5036609 Cumulative Update for .NET Framework 4.8 for Windows 10, version 1607 and Windows Server 2016 - Microsoft Support	CVE-2024-21409	Remote Code Execution	Important	No	No	2
5037037	高危	April 9, 2024- KB5037037 Cumulative Update for .NET Framework 3.5, 4.8 and 4.8.1 for Windows 11, version 21H2 - Microsoft Support	CVE-2024-21409	Remote Code Execution	Important	No	No	2

5037035	高危	April 9, 2024- KB5037035 Cumulative Update for .NET Framework 3.5, 4.8 and 4.8.1 for Windows 10 Version 21H2 - Microsoft Support	CVE-2024-21409	Remote Code Execution	Important	No	No	2
5037041	高危	April 9, 2024- Security and Quality Rollup for .NET Framework 2.0, 3.0, 3.5 SP1, 4.6.2 for Windows Server 2008 SP2 (KB5037041) - Microsoft Support	CVE-2024-21409	Remote Code Execution	Important	No	No	2
5037033	高危	April 9, 2024- KB5037033 Cumulative Update for .NET Framework 3.5, 4.8 and 4.8.1	CVE-2024-21409	Remote Code Execution	Important	No	No	2

		for Windows Server 2022 - Microsoft Support						
5037039	高危	April 9, 2024- Security and Quality Rollup for .NET Framework 3.5, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Windows Server 2012 (KB5037039) - Microsoft Support	CVE-2024-21409	Remote Code Execution	Important	No	No	2
5037038	高危	April 9, 2024- Security and Quality Rollup for .NET Framework 3.5.1, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Windows	CVE-2024-21409	Remote Code Execution	Important	No	No	2

		Server 2008 R2 SP1 (KB5037038) - Microsoft Support						
5036620	高危	April 9, 2024- KB5036620 Cumulative Update for .NET Framework 3.5 and 4.8.1 for Windows 11, version 22H2 and Windows 11, version 23H2 - Microsoft Support	CVE-2024-21409	Remote Code Execution	Important	No	No	2
5037034	高危	April 9, 2024- KB5037034 Cumulative Update for .NET Framework 3.5, 4.7.2 and 4.8 for Windows 10, version 1809 and Windows Server	CVE-2024-21409	Remote Code Execution	Important	No	No	2

		2019 - Microsoft Support						
5037127	高危	April 9, 2024- Security Only Update for .NET Framework 3.5.1, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Windows Server 2008 R2 SP1 (KB5037127) - Microsoft Support	CVE-2024-21409	Remote Code Execution	Important	No	No	2
5037040	高危	April 9, 2024- Security and Quality Rollup for .NET Framework 3.5, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Windows Server 2012 R2 (KB5037040	CVE-2024-21409	Remote Code Execution	Important	No	No	2

		) - Microsoft Support						
5002583	高危	Description of the security update for SharePoint Enterprise Server 2016: April 9, 2024 (KB5002583) - Microsoft Support	CVE-2024-26251	Spoofing	Important	No	No	2
5037128	高危	April 9, 2024- Security Only Update for .NET Framework 2.0, 3.0, 3.5 SP1, 4.6.2 for Windows Server 2008 SP2 (KB5037128) - Microsoft Support	CVE-2024-21409	Remote Code Execution	Important	No	No	2
5037036	高危	April 9, 2024- KB5037036 Cumulative Update for .NET Framework 3.5, 4.8	CVE-2024-21409	Remote Code Execution	Important	No	No	2

		and 4.8.1 for Windows 10 Version 22H2 - Microsoft Support						

本月发布 10 个一般性更新补丁。

KBID	奇安信集团级别	详细信息
5002050	其他功能性补丁	Office 2016 更新程序
5002340	其他功能性补丁	Office 2016 更新程序
5002388	其他功能性补丁	Office 2016 更新程序
5002525	其他功能性补丁	Office 2016 更新程序
5002545	其他功能性补丁	Office 2016 更新程序
5002568	其他功能性补丁	Office 2016 更新程序
5002571	其他功能性补丁	Office 2016 更新程序
5002572	其他功能性补丁	Office 2016 更新程序
5002574	其他功能性补丁	Office 2016 更新程序
5002577	其他功能性补丁	Office 2016 更新程序

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