

奇安信集团 2023 年 7 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

2023 年 7 月 12 日

目 录

第 1 章 安全通告.....	2
第 2 章 重点关注补丁.....	3
第 3 章 已知问题和特殊调整.....	8
第 4 章 漏洞补丁详细列表.....	9
第 5 章 参考链接.....	69

文档信息

文档名称	奇安信集团 2023 年 7 月补丁库更新通告		
文档编号	Qi An Xin Group-MSPatch-2023-0701		
发布日期	2023-07-12	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:2023.07.12.1,V10 版本:2023.07.12.1000)已发布，本次更新推送了 31 个微软安全补丁，修复了 112 个安全漏洞，其中 9 个微软官方评级为“严重(Critical)”，103 个评级为“重要(Important)”，这些漏洞影响 Windows、.NET Framework、Internet Explorer、Office 等产品。

第2章 重点关注补丁

本月有 18 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
5028167	CVE-2023-32046	Elevation of Privilege	Important	No	Yes	Exploitation Detected
5028166						
5028233						
5028171						
5028232						
5028168						
5028222						
5028182						
5028223						
5028224						
5028169						
5028240						
5028185						
5028186						
5028226						
5028228						
5028166	CVE-2023-35315	Remote Code Execution	Critical	No	No	Exploitation Less Likely
5028171						
5028168						
5028182						
5028185	CVE-2023-35365	Remote Code Execution	Critical	No	No	Exploitation Less Likely
5028166						
5028233						
5028171						
5028232						
5028168						
5028222						
5028182						

5028223						
5028224						
5028169						
5028240						
5028185						
5028186						
5028226						
5028228						
5028166	CVE-2023-32049	Security Feature Bypass	Important	No	Yes	Exploitation Detected
5028171						
5028168						
5028182						
5028169						
5028185						
5028166	CVE-2023-32057	Remote Code Execution	Critical	No	No	Exploitation Less Likely
5028233						
5028171						
5028232						
5028168						
5028222						
5028182						
5028223						
5028224						
5028169						
5028240						
5028185						
5028186						
5028226						
5028228						
5028166	CVE-2023-36874	Elevation of Privilege	Important	No	Yes	Exploitation Detected
5028233						
5028171						
5028232						
5028168						
5028222						
5028182						
5028223						
5028169						
5028240						
5028185						
5028186						

5028226						
5028228						
5028166	CVE-2023-35297	Remote Code Execution	Critical	No	No	Exploitation Less Likely
5028233						
5028171						
5028232						
5028168						
5028222						
5028182						
5028223						
5028224						
5028169						
5028240						
5028185						
5028186						
5028226						
5028228						
5028166						
5028233						
5028171						
5028232						
5028168						
5028222						
5028182						
5028223						
5028224						
5028169						
5028240						
5028185						
5028186						
5028226						
5028228						
5028166	CVE-2023-35312	Elevation of Privilege	Important	No	No	Exploitation More Likely
5028233						
5028171						
5028232						
5028168						
5028182						
5028223						
5028224						
5028169						

5028240						
5028185						
5028186						
5028228						
5028166	CVE-2023-21526	Information Disclosure	Important	No	No	Exploitation More Likely
5028233						
5028171						
5028232						
5028168						
5028222						
5028182						
5028223						
5028224						
5028169						
5028240						
5028185						
5028186						
5028226						
5028228						
5028166						
5028233						
5028171						
5028232						
5028168						
5028222						
5028182						
5028223						
5028224						
5028169						
5028240						
5028185						
5028186						
5028226						
5028228						
5028166	CVE-2023-36871	Security Feature Bypass	Important	No	No	Exploitation More Likely
5028171						
5028168						
5028182						
5028169						
5028185						
5028186						

5028166	ADV230001	Defense in Depth	None	No	Yes	Exploitation Detected
5028233						
5028171						
5028232						
5028168						
5028222						
5028182						
5028223						
5028224						
5028169						
5028240						
5028185						
5028186						
5028226						
5028228						
5028233	CVE-2023-35352	Security Feature Bypass	Critical	No	No	Exploitation More Likely
5028171						
5028232						
5028168						
5028223						
5028169						
5028228						
5002427	CVE-2023-35311	Security Feature Bypass	Important	No	Yes	Exploitation Detected
5002432						
5002425	CVE-2023-33160	Remote Code Execution	Critical	No	No	Exploitation Less Likely
5002425	CVE-2023-33134	Remote Code Execution	Important	No	No	Exploitation More Likely
5002425	CVE-2023-33157	Remote Code Execution	Critical	No	No	Exploitation More Likely

第3章 已知问题和特殊调整

本月暂无已知问题和特殊调整。

第4章 漏洞补丁详细列表

本月微软发布的系统安全更新补丁共 15 个，详细列表如下：

KBID	奇安信集团级别	补丁名称	CVE 编号	漏洞的影响	漏洞等级	公开披露	已受攻击	漏洞的可利用性
5028166	高危	July 11, 2023—KB5028166 (OS Builds 19044.3208 and 19045.3208) – Microsoft Support for Windows 10 Enterprise and Education, version 21H2, Windows 10 IoT Enterprise, version 21H2, Windows 10 Enterprise Multi-Session,	CVE-2023-35315	Remote Code Execution	Critical	No	No	2
			CVE-2023-33174	Information Disclosure	Important	No	No	2
			CVE-2023-35316	Information Disclosure	Important	No	No	2
			CVE-2023-35326	Information Disclosure	Important	No	No	2
			CVE-2023-32035	Denial of Service	Important	No	No	2
			CVE-2023-35343	Remote Code Execution	Important	No	No	2
			CVE-2023-35302	Remote Code Execution	Important	No	No	2
			CVE-2023-35337	Elevation of Privilege	Important	No	No	2
			CVE-2023-35308	Security Feature Bypass	Important	No	No	2
			CVE-2023-35296	Information Disclosure	Important	No	No	2
			CVE-2023-32041	Information Disclosure	Important	No	No	2
			CVE-2023-35358	Elevation of Privilege	Important	No	No	2
			CVE-2023-35341	Information Disclosure	Important	No	No	2
CVE-2023-33172	Denial of Service	Important	No	No	2			

version 21H2, Windows 10, version 22H2, all editions	CVE-2023-32034	Denial of Service	Important	No	No	2
	CVE-2023-33168	Denial of Service	Important	No	No	2
	CVE-2023-35320	Elevation of Privilege	Important	No	No	2
	CVE-2023-32042	Information Disclosure	Important	No	No	2
	CVE-2023-35365	Remote Code Execution	Critical	No	No	2
	CVE-2023-35342	Elevation of Privilege	Important	No	No	2
	CVE-2023-32085	Information Disclosure	Important	No	No	2
	CVE-2023-32049	Security Feature Bypass	Important	No	Yes	0
	CVE-2023-21756	Elevation of Privilege	Important	No	No	2
	CVE-2023-35313	Remote Code Execution	Important	No	No	2
	CVE-2023-35325	Information Disclosure	Important	No	No	2
	CVE-2023-35306	Information Disclosure	Important	No	No	2
	CVE-2023-35324	Information Disclosure	Important	No	No	2
	CVE-2023-35356	Elevation of Privilege	Important	No	No	2
	CVE-2023-35314	Denial of Service	Important	No	No	2
	CVE-2023-35319	Denial of Service	Important	No	No	2
	CVE-2023-32040	Information Disclosure	Important	No	No	2
	CVE-2023-33173	Denial of Service	Important	No	No	2
	CVE-2023-32057	Remote Code Execution	Critical	No	No	2
	CVE-2023-35360	Elevation of Privilege	Important	No	No	2

			CVE-2023-32045	Denial of Service	Important	No	No	2
			CVE-2023-35303	Remote Code Execution	Important	No	No	2
			CVE-2023-35329	Denial of Service	Important	No	No	2
			CVE-2023-35353	Elevation of Privilege	Important	No	No	2
			CVE-2023-36874	Elevation of Privilege	Important	No	Yes	0
			CVE-2023-35297	Remote Code Execution	Critical	No	No	2
			CVE-2023-33166	Denial of Service	Important	No	No	2
			CVE-2023-32056	Elevation of Privilege	Important	No	No	2
			CVE-2023-35299	Elevation of Privilege	Important	No	No	2
			CVE-2023-32044	Denial of Service	Important	No	No	2
			CVE-2023-32053	Elevation of Privilege	Important	No	No	2
			CVE-2023-35340	Elevation of Privilege	Important	No	No	2
			CVE-2023-35367	Remote Code Execution	Critical	No	No	2
			CVE-2023-32039	Information Disclosure	Important	No	No	2
			CVE-2023-32037	Information Disclosure	Important	No	No	2
			CVE-2023-35318	Denial of Service	Important	No	No	2
			CVE-2023-35312	Elevation of Privilege	Important	No	No	1
			CVE-2023-32046	Elevation of Privilege	Important	No	Yes	0
			CVE-2023-35364	Elevation of Privilege	Important	No	No	2
			CVE-2023-35300	Remote Code Execution	Important	No	No	2

			CVE-2023-33155	Elevation of Privilege	Important	No	No	2
			ADV230002	Security Feature Bypass	Important	No	No	2
			CVE-2023-21526	Information Disclosure	Important	No	No	1
			CVE-2023-32055	Elevation of Privilege	Important	No	No	2
			CVE-2023-32043	Security Feature Bypass	Important	No	No	2
			CVE-2023-35366	Remote Code Execution	Critical	No	No	2
			CVE-2023-33164	Denial of Service	Important	No	No	2
			CVE-2023-33169	Denial of Service	Important	No	No	2
			CVE-2023-35305	Elevation of Privilege	Important	No	No	2
			CVE-2023-35336	Security Feature Bypass	Important	No	No	2
			CVE-2023-35347	Elevation of Privilege	Important	No	No	2
			CVE-2023-35330	Denial of Service	Important	No	No	2
			CVE-2023-36871	Security Feature Bypass	Important	No	No	1
			CVE-2023-35339	Denial of Service	Important	No	No	2
			CVE-2023-35357	Elevation of Privilege	Important	No	No	2
			CVE-2023-35309	Remote Code Execution	Important	No	No	2
			CVE-2023-32038	Remote Code Execution	Important	No	No	2
			CVE-2023-35338	Denial of Service	Important	No	No	2
			CVE-2023-35363	Elevation of Privilege	Important	No	No	2

			CVE-2023-35304	Elevation of Privilege	Important	No	No	2
			CVE-2023-33154	Elevation of Privilege	Important	No	No	2
			CVE-2023-35332	Security Feature Bypass	Important	No	No	2
			CVE-2023-33167	Denial of Service	Important	No	No	2
			CVE-2023-35362	Elevation of Privilege	Important	No	No	2
			CVE-2023-32054	Elevation of Privilege	Important	No	No	2
			CVE-2023-35328	Elevation of Privilege	Important	No	No	2
			ADV230001	Defense in Depth	None	No	Yes	0
			CVE-2023-35361	Elevation of Privilege	Important	No	No	2
5028233	高危	July 11, 2023—KB5028233 (Security-only update) – Microsoft Support for Windows Server 2012, Windows Embedded Standard 8	CVE-2023-35366	Remote Code Execution	Critical	No	No	2
			CVE-2023-33164	Denial of Service	Important	No	No	2
			CVE-2023-35365	Remote Code Execution	Critical	No	No	2
			CVE-2023-32053	Elevation of Privilege	Important	No	No	2
			CVE-2023-33169	Denial of Service	Important	No	No	2
			CVE-2023-35340	Elevation of Privilege	Important	No	No	2
			CVE-2023-35344	Remote Code Execution	Important	No	No	2
			CVE-2023-35367	Remote Code Execution	Critical	No	No	2
			CVE-2023-35331	Denial of Service	Important	No	No	2
			CVE-2023-35330	Denial of Service	Important	No	No	2
			CVE-2023-32039	Information Disclosure	Important	No	No	2

		CVE-2023-33163	Remote Code Execution	Important	No	No	2
		CVE-2023-35342	Elevation of Privilege	Important	No	No	2
		CVE-2023-32085	Information Disclosure	Important	No	No	2
		CVE-2023-35346	Remote Code Execution	Important	No	No	2
		CVE-2023-33174	Information Disclosure	Important	No	No	2
		CVE-2023-35316	Information Disclosure	Important	No	No	2
		CVE-2023-35318	Denial of Service	Important	No	No	2
		CVE-2023-21756	Elevation of Privilege	Important	No	No	2
		CVE-2023-35352	Security Feature Bypass	Critical	No	No	1
		ADV230001	Defense in Depth	None	No	Yes	0
		CVE-2023-35322	Remote Code Execution	Important	No	No	2
		CVE-2023-35312	Elevation of Privilege	Important	No	No	1
		CVE-2023-35309	Remote Code Execution	Important	No	No	2
		CVE-2023-32038	Remote Code Execution	Important	No	No	2
		CVE-2023-35325	Information Disclosure	Important	No	No	2
		CVE-2023-32035	Denial of Service	Important	No	No	2
		CVE-2023-35317	Elevation of Privilege	Important	No	No	2
		CVE-2023-35302	Remote Code Execution	Important	No	No	2
		CVE-2023-35338	Denial of Service	Important	No	No	2
		CVE-2023-35306	Information Disclosure	Important	No	No	2

			CVE-2023-35351	Remote Code Execution	Important	No	No	2
			CVE-2023-35324	Information Disclosure	Important	No	No	2
			CVE-2023-35296	Information Disclosure	Important	No	No	2
			CVE-2023-35314	Denial of Service	Important	No	No	2
			CVE-2023-32033	Remote Code Execution	Important	No	No	2
			CVE-2023-32046	Elevation of Privilege	Important	No	Yes	0
			CVE-2023-35319	Denial of Service	Important	No	No	2
			CVE-2023-32054	Elevation of Privilege	Important	No	No	2
			CVE-2023-32040	Information Disclosure	Important	No	No	2
			CVE-2023-32057	Remote Code Execution	Critical	No	No	2
			CVE-2023-35360	Elevation of Privilege	Important	No	No	2
			CVE-2023-35300	Remote Code Execution	Important	No	No	2
			CVE-2023-35350	Remote Code Execution	Important	No	No	2
			CVE-2023-35303	Remote Code Execution	Important	No	No	2
			CVE-2023-32045	Denial of Service	Important	No	No	2
			CVE-2023-35341	Information Disclosure	Important	No	No	2
			CVE-2023-33154	Elevation of Privilege	Important	No	No	2
			CVE-2023-33173	Denial of Service	Important	No	No	2
			CVE-2023-33172	Denial of Service	Important	No	No	2
			CVE-2023-32034	Denial of Service	Important	No	No	2

			CVE-2023-35329	Denial of Service	Important	No	No	2
			ADV230002	Security Feature Bypass	Important	No	No	2
			CVE-2023-33168	Denial of Service	Important	No	No	2
			CVE-2023-21526	Information Disclosure	Important	No	No	1
			CVE-2023-36874	Elevation of Privilege	Important	No	Yes	0
			CVE-2023-35345	Remote Code Execution	Important	No	No	2
			CVE-2023-32055	Elevation of Privilege	Important	No	No	2
			CVE-2023-35310	Remote Code Execution	Important	No	No	2
			CVE-2023-35332	Security Feature Bypass	Important	No	No	2
			CVE-2023-35297	Remote Code Execution	Critical	No	No	2
			CVE-2023-35321	Denial of Service	Important	No	No	2
			CVE-2023-32043	Security Feature Bypass	Important	No	No	2
			CVE-2023-33167	Denial of Service	Important	No	No	2
			CVE-2023-33166	Denial of Service	Important	No	No	2
			CVE-2023-35299	Elevation of Privilege	Important	No	No	2
			CVE-2023-32044	Denial of Service	Important	No	No	2
			CVE-2023-35328	Elevation of Privilege	Important	No	No	2
			CVE-2023-32042	Information Disclosure	Important	No	No	2
			CVE-2023-35361	Elevation of Privilege	Important	No	No	2

5028171	高危	July 11, 2023— KB5028171 (OS Build 20348.1850) - Microsoft Support for Windows Server 2022	CVE-2023-35344	Remote Code Execution	Important	No	No	2
			CVE-2023-35315	Remote Code Execution	Critical	No	No	2
			CVE-2023-33163	Remote Code Execution	Important	No	No	2
			CVE-2023-33174	Information Disclosure	Important	No	No	2
			CVE-2023-35316	Information Disclosure	Important	No	No	2
			CVE-2023-35326	Information Disclosure	Important	No	No	2
			CVE-2023-32035	Denial of Service	Important	No	No	2
			CVE-2023-35343	Remote Code Execution	Important	No	No	2
			CVE-2023-35302	Remote Code Execution	Important	No	No	2
			CVE-2023-35337	Elevation of Privilege	Important	No	No	2
			CVE-2023-35308	Security Feature Bypass	Important	No	No	2
			CVE-2023-35296	Information Disclosure	Important	No	No	2
			CVE-2023-32041	Information Disclosure	Important	No	No	2
			CVE-2023-35350	Remote Code Execution	Important	No	No	2
			CVE-2023-35358	Elevation of Privilege	Important	No	No	2
			CVE-2023-35341	Information Disclosure	Important	No	No	2
			CVE-2023-33172	Denial of Service	Important	No	No	2
			CVE-2023-32034	Denial of Service	Important	No	No	2
			CVE-2023-33168	Denial of Service	Important	No	No	2
			CVE-2023-35345	Remote Code Execution	Important	No	No	2

			CVE-2023-35320	Elevation of Privilege	Important	No	No	2
			CVE-2023-32042	Information Disclosure	Important	No	No	2
			CVE-2023-35352	Security Feature Bypass	Critical	No	No	1
			CVE-2023-35365	Remote Code Execution	Critical	No	No	2
			CVE-2023-35342	Elevation of Privilege	Important	No	No	2
			CVE-2023-32085	Information Disclosure	Important	No	No	2
			CVE-2023-32049	Security Feature Bypass	Important	No	Yes	0
			CVE-2023-21756	Elevation of Privilege	Important	No	No	2
			CVE-2023-35323	Remote Code Execution	Important	No	No	2
			CVE-2023-35313	Remote Code Execution	Important	No	No	2
			CVE-2023-35325	Information Disclosure	Important	No	No	2
			CVE-2023-35306	Information Disclosure	Important	No	No	2
			CVE-2023-32083	Information Disclosure	Important	No	No	2
			CVE-2023-35356	Elevation of Privilege	Important	No	No	2
			CVE-2023-35324	Information Disclosure	Important	No	No	2
			CVE-2023-35314	Denial of Service	Important	No	No	2
			CVE-2023-35319	Denial of Service	Important	No	No	2
			CVE-2023-32040	Information Disclosure	Important	No	No	2
			CVE-2023-32057	Remote Code Execution	Critical	No	No	2

			CVE-2023-35360	Elevation of Privilege	Important	No	No	2
			CVE-2023-32045	Denial of Service	Important	No	No	2
			CVE-2023-33173	Denial of Service	Important	No	No	2
			CVE-2023-35303	Remote Code Execution	Important	No	No	2
			CVE-2023-35329	Denial of Service	Important	No	No	2
			CVE-2023-35353	Elevation of Privilege	Important	No	No	2
			CVE-2023-36874	Elevation of Privilege	Important	No	Yes	0
			CVE-2023-35297	Remote Code Execution	Critical	No	No	2
			CVE-2023-35310	Remote Code Execution	Important	No	No	2
			CVE-2023-33166	Denial of Service	Important	No	No	2
			CVE-2023-32056	Elevation of Privilege	Important	No	No	2
			CVE-2023-35299	Elevation of Privilege	Important	No	No	2
			CVE-2023-32044	Denial of Service	Important	No	No	2
			CVE-2023-32053	Elevation of Privilege	Important	No	No	2
			CVE-2023-35340	Elevation of Privilege	Important	No	No	2
			CVE-2023-35367	Remote Code Execution	Critical	No	No	2
			CVE-2023-32039	Information Disclosure	Important	No	No	2
			CVE-2023-32037	Information Disclosure	Important	No	No	2
			CVE-2023-35318	Denial of Service	Important	No	No	2
			CVE-2023-35312	Elevation of Privilege	Important	No	No	1

			CVE-2023-35348	Security Feature Bypass	Important	No	No	2
			CVE-2023-35317	Elevation of Privilege	Important	No	No	2
			CVE-2023-32084	Denial of Service	Important	No	No	2
			CVE-2023-32046	Elevation of Privilege	Important	No	Yes	0
			CVE-2023-35364	Elevation of Privilege	Important	No	No	2
			CVE-2023-35300	Remote Code Execution	Important	No	No	2
			CVE-2023-33155	Elevation of Privilege	Important	No	No	2
			ADV230002	Security Feature Bypass	Important	No	No	2
			CVE-2023-21526	Information Disclosure	Important	No	No	1
			CVE-2023-32055	Elevation of Privilege	Important	No	No	2
			CVE-2023-32043	Security Feature Bypass	Important	No	No	2
			CVE-2023-35366	Remote Code Execution	Critical	No	No	2
			CVE-2023-33164	Denial of Service	Important	No	No	2
			CVE-2023-33169	Denial of Service	Important	No	No	2
			CVE-2023-35305	Elevation of Privilege	Important	No	No	2
			CVE-2023-35336	Security Feature Bypass	Important	No	No	2
			CVE-2023-35347	Elevation of Privilege	Important	No	No	2
			CVE-2023-35331	Denial of Service	Important	No	No	2
			CVE-2023-35330	Denial of Service	Important	No	No	2

			CVE-2023-36871	Security Feature Bypass	Important	No	No	1
			CVE-2023-35339	Denial of Service	Important	No	No	2
			CVE-2023-35346	Remote Code Execution	Important	No	No	2
			CVE-2023-35357	Elevation of Privilege	Important	No	No	2
			CVE-2023-35322	Remote Code Execution	Important	No	No	2
			CVE-2023-35309	Remote Code Execution	Important	No	No	2
			CVE-2023-32038	Remote Code Execution	Important	No	No	2
			CVE-2023-35338	Denial of Service	Important	No	No	2
			CVE-2023-35363	Elevation of Privilege	Important	No	No	2
			CVE-2023-35298	Denial of Service	Important	No	No	2
			CVE-2023-35351	Remote Code Execution	Important	No	No	2
			CVE-2023-32033	Remote Code Execution	Important	No	No	2
			CVE-2023-35304	Elevation of Privilege	Important	No	No	2
			CVE-2023-33154	Elevation of Privilege	Important	No	No	2
			CVE-2023-35332	Security Feature Bypass	Important	No	No	2
			CVE-2023-33167	Denial of Service	Important	No	No	2
			CVE-2023-35321	Denial of Service	Important	No	No	2
			CVE-2023-35362	Elevation of Privilege	Important	No	No	2
			CVE-2023-32054	Elevation of Privilege	Important	No	No	2

			CVE-2023-35328	Elevation of Privilege	Important	No	No	2
			ADV230001	Defense in Depth	None	No	Yes	0
			CVE-2023-35361	Elevation of Privilege	Important	No	No	2
5028232	高危	July 11, 2023—KB5028232 (Monthly Rollup) – Microsoft Support for Windows Server 2012, Windows Embedded 8 Standard	CVE-2023-35366	Remote Code Execution	Critical	No	No	2
			CVE-2023-33164	Denial of Service	Important	No	No	2
			CVE-2023-35365	Remote Code Execution	Critical	No	No	2
			CVE-2023-32053	Elevation of Privilege	Important	No	No	2
			CVE-2023-33169	Denial of Service	Important	No	No	2
			CVE-2023-35340	Elevation of Privilege	Important	No	No	2
			CVE-2023-35344	Remote Code Execution	Important	No	No	2
			CVE-2023-35367	Remote Code Execution	Critical	No	No	2
			CVE-2023-35331	Denial of Service	Important	No	No	2
			CVE-2023-35330	Denial of Service	Important	No	No	2
			CVE-2023-32039	Information Disclosure	Important	No	No	2
			CVE-2023-33163	Remote Code Execution	Important	No	No	2
			CVE-2023-35342	Elevation of Privilege	Important	No	No	2
			CVE-2023-32085	Information Disclosure	Important	No	No	2
			CVE-2023-35346	Remote Code Execution	Important	No	No	2
			CVE-2023-33174	Information Disclosure	Important	No	No	2
			CVE-2023-35316	Information Disclosure	Important	No	No	2

			CVE-2023-35318	Denial of Service	Important	No	No	2
			CVE-2023-21756	Elevation of Privilege	Important	No	No	2
			CVE-2023-35352	Security Feature Bypass	Critical	No	No	1
			ADV230001	Defense in Depth	None	No	Yes	0
			CVE-2023-35322	Remote Code Execution	Important	No	No	2
			CVE-2023-35312	Elevation of Privilege	Important	No	No	1
			CVE-2023-35309	Remote Code Execution	Important	No	No	2
			CVE-2023-32038	Remote Code Execution	Important	No	No	2
			CVE-2023-35325	Information Disclosure	Important	No	No	2
			CVE-2023-32035	Denial of Service	Important	No	No	2
			CVE-2023-35317	Elevation of Privilege	Important	No	No	2
			CVE-2023-35302	Remote Code Execution	Important	No	No	2
			CVE-2023-35338	Denial of Service	Important	No	No	2
			CVE-2023-35306	Information Disclosure	Important	No	No	2
			CVE-2023-35351	Remote Code Execution	Important	No	No	2
			CVE-2023-35324	Information Disclosure	Important	No	No	2
			CVE-2023-35296	Information Disclosure	Important	No	No	2
			CVE-2023-35314	Denial of Service	Important	No	No	2
			CVE-2023-32033	Remote Code Execution	Important	No	No	2
			CVE-2023-32046	Elevation of Privilege	Important	No	Yes	0

		CVE-2023-35319	Denial of Service	Important	No	No	2
		CVE-2023-32054	Elevation of Privilege	Important	No	No	2
		CVE-2023-32040	Information Disclosure	Important	No	No	2
		CVE-2023-32057	Remote Code Execution	Critical	No	No	2
		CVE-2023-35360	Elevation of Privilege	Important	No	No	2
		CVE-2023-35300	Remote Code Execution	Important	No	No	2
		CVE-2023-35350	Remote Code Execution	Important	No	No	2
		CVE-2023-35303	Remote Code Execution	Important	No	No	2
		CVE-2023-32045	Denial of Service	Important	No	No	2
		CVE-2023-35341	Information Disclosure	Important	No	No	2
		CVE-2023-33154	Elevation of Privilege	Important	No	No	2
		CVE-2023-33173	Denial of Service	Important	No	No	2
		CVE-2023-33172	Denial of Service	Important	No	No	2
		CVE-2023-32034	Denial of Service	Important	No	No	2
		CVE-2023-35329	Denial of Service	Important	No	No	2
		ADV230002	Security Feature Bypass	Important	No	No	2
		CVE-2023-33168	Denial of Service	Important	No	No	2
		CVE-2023-21526	Information Disclosure	Important	No	No	1
		CVE-2023-36874	Elevation of Privilege	Important	No	Yes	0
		CVE-2023-35345	Remote Code Execution	Important	No	No	2

			CVE-2023-32055	Elevation of Privilege	Important	No	No	2
			CVE-2023-35310	Remote Code Execution	Important	No	No	2
			CVE-2023-35332	Security Feature Bypass	Important	No	No	2
			CVE-2023-35297	Remote Code Execution	Critical	No	No	2
			CVE-2023-35321	Denial of Service	Important	No	No	2
			CVE-2023-32043	Security Feature Bypass	Important	No	No	2
			CVE-2023-33167	Denial of Service	Important	No	No	2
			CVE-2023-33166	Denial of Service	Important	No	No	2
			CVE-2023-35299	Elevation of Privilege	Important	No	No	2
			CVE-2023-32044	Denial of Service	Important	No	No	2
			CVE-2023-35328	Elevation of Privilege	Important	No	No	2
			CVE-2023-32042	Information Disclosure	Important	No	No	2
			CVE-2023-35361	Elevation of Privilege	Important	No	No	2
5028168	高危	July 11, 2023— KB5028168 (OS Build 17763.464 5) – Microsoft Support for Win 10 Ent LTSC v2019, Win	CVE-2023-35344	Remote Code Execution	Important	No	No	2
			CVE-2023-35315	Remote Code Execution	Critical	No	No	2
			CVE-2023-33163	Remote Code Execution	Important	No	No	2
			CVE-2023-33174	Information Disclosure	Important	No	No	2
			CVE-2023-35316	Information Disclosure	Important	No	No	2
			CVE-2023-35326	Information Disclosure	Important	No	No	2

	10 IoT Ent LTSC v2019, Win dows 10 IoT Core 2019 LTSC, Wind ows Server 2019	CVE-2023-32035	Denial of Service	Important	No	No	2
		CVE-2023-35343	Remote Code Execution	Important	No	No	2
		CVE-2023-35302	Remote Code Execution	Important	No	No	2
		CVE-2023-35308	Security Feature Bypass	Important	No	No	2
		CVE-2023-35296	Information Disclosure	Important	No	No	2
		CVE-2023-32041	Information Disclosure	Important	No	No	2
		CVE-2023-35350	Remote Code Execution	Important	No	No	2
		CVE-2023-35358	Elevation of Privilege	Important	No	No	2
		CVE-2023-35341	Information Disclosure	Important	No	No	2
		CVE-2023-33172	Denial of Service	Important	No	No	2
		CVE-2023-32034	Denial of Service	Important	No	No	2
		CVE-2023-33168	Denial of Service	Important	No	No	2
		CVE-2023-35345	Remote Code Execution	Important	No	No	2
		CVE-2023-35320	Elevation of Privilege	Important	No	No	2
		CVE-2023-32042	Information Disclosure	Important	No	No	2
		CVE-2023-35352	Security Feature Bypass	Critical	No	No	1
		CVE-2023-35365	Remote Code Execution	Critical	No	No	2
		CVE-2023-35342	Elevation of Privilege	Important	No	No	2
		CVE-2023-32085	Information Disclosure	Important	No	No	2

			CVE-2023-32049	Security Feature Bypass	Important	No	Yes	0
			CVE-2023-21756	Elevation of Privilege	Important	No	No	2
			CVE-2023-35313	Remote Code Execution	Important	No	No	2
			CVE-2023-35325	Information Disclosure	Important	No	No	2
			CVE-2023-35306	Information Disclosure	Important	No	No	2
			CVE-2023-32083	Information Disclosure	Important	No	No	2
			CVE-2023-35356	Elevation of Privilege	Important	No	No	2
			CVE-2023-35324	Information Disclosure	Important	No	No	2
			CVE-2023-35314	Denial of Service	Important	No	No	2
			CVE-2023-35319	Denial of Service	Important	No	No	2
			CVE-2023-32040	Information Disclosure	Important	No	No	2
			CVE-2023-32057	Remote Code Execution	Critical	No	No	2
			CVE-2023-35360	Elevation of Privilege	Important	No	No	2
			CVE-2023-32045	Denial of Service	Important	No	No	2
			CVE-2023-33173	Denial of Service	Important	No	No	2
			CVE-2023-35303	Remote Code Execution	Important	No	No	2
			CVE-2023-35329	Denial of Service	Important	No	No	2
			CVE-2023-35353	Elevation of Privilege	Important	No	No	2
			CVE-2023-36874	Elevation of Privilege	Important	No	Yes	0
			CVE-2023-35297	Remote Code Execution	Critical	No	No	2

		CVE-2023-35310	Remote Code Execution	Important	No	No	2
		CVE-2023-33166	Denial of Service	Important	No	No	2
		CVE-2023-32056	Elevation of Privilege	Important	No	No	2
		CVE-2023-35299	Elevation of Privilege	Important	No	No	2
		CVE-2023-32044	Denial of Service	Important	No	No	2
		CVE-2023-32053	Elevation of Privilege	Important	No	No	2
		CVE-2023-35340	Elevation of Privilege	Important	No	No	2
		CVE-2023-35367	Remote Code Execution	Critical	No	No	2
		CVE-2023-32039	Information Disclosure	Important	No	No	2
		CVE-2023-32037	Information Disclosure	Important	No	No	2
		CVE-2023-35318	Denial of Service	Important	No	No	2
		CVE-2023-35312	Elevation of Privilege	Important	No	No	1
		CVE-2023-35348	Security Feature Bypass	Important	No	No	2
		CVE-2023-35317	Elevation of Privilege	Important	No	No	2
		CVE-2023-32084	Denial of Service	Important	No	No	2
		CVE-2023-32046	Elevation of Privilege	Important	No	Yes	0
		CVE-2023-35364	Elevation of Privilege	Important	No	No	2
		CVE-2023-35300	Remote Code Execution	Important	No	No	2
		CVE-2023-33155	Elevation of Privilege	Important	No	No	2

			ADV230002	Security Feature Bypass	Important	No	No	2
			CVE-2023-21526	Information Disclosure	Important	No	No	1
			CVE-2023-32055	Elevation of Privilege	Important	No	No	2
			CVE-2023-32043	Security Feature Bypass	Important	No	No	2
			CVE-2023-35366	Remote Code Execution	Critical	No	No	2
			CVE-2023-33164	Denial of Service	Important	No	No	2
			CVE-2023-33169	Denial of Service	Important	No	No	2
			CVE-2023-35305	Elevation of Privilege	Important	No	No	2
			CVE-2023-35336	Security Feature Bypass	Important	No	No	2
			CVE-2023-35331	Denial of Service	Important	No	No	2
			CVE-2023-35330	Denial of Service	Important	No	No	2
			CVE-2023-36871	Security Feature Bypass	Important	No	No	1
			CVE-2023-35339	Denial of Service	Important	No	No	2
			CVE-2023-35346	Remote Code Execution	Important	No	No	2
			CVE-2023-35357	Elevation of Privilege	Important	No	No	2
			CVE-2023-35322	Remote Code Execution	Important	No	No	2
			CVE-2023-35309	Remote Code Execution	Important	No	No	2
			CVE-2023-32038	Remote Code Execution	Important	No	No	2
			CVE-2023-35338	Denial of Service	Important	No	No	2

			CVE-2023-35363	Elevation of Privilege	Important	No	No	2
			CVE-2023-35351	Remote Code Execution	Important	No	No	2
			CVE-2023-32033	Remote Code Execution	Important	No	No	2
			CVE-2023-35304	Elevation of Privilege	Important	No	No	2
			CVE-2023-33154	Elevation of Privilege	Important	No	No	2
			CVE-2023-35332	Security Feature Bypass	Important	No	No	2
			CVE-2023-33167	Denial of Service	Important	No	No	2
			CVE-2023-35321	Denial of Service	Important	No	No	2
			CVE-2023-35362	Elevation of Privilege	Important	No	No	2
			CVE-2023-32054	Elevation of Privilege	Important	No	No	2
			CVE-2023-35328	Elevation of Privilege	Important	No	No	2
			ADV230001	Defense in Depth	None	No	Yes	0
			CVE-2023-35361	Elevation of Privilege	Important	No	No	2
5028222	高危	July 11, 2023—KB5028222 (Monthly Rollup) – Microsoft Support for Windows Server 2008 Datacenter ESU, Windo	CVE-2023-35366	Remote Code Execution	Critical	No	No	2
			CVE-2023-33164	Denial of Service	Important	No	No	2
			CVE-2023-35365	Remote Code Execution	Critical	No	No	2
			CVE-2023-33169	Denial of Service	Important	No	No	2
			CVE-2023-35340	Elevation of Privilege	Important	No	No	2
			CVE-2023-35344	Remote Code Execution	Important	No	No	2
			CVE-2023-35367	Remote Code Execution	Critical	No	No	2

	ws Server 2008	CVE-2023-32042	Information Disclosure	Important	No	No	2
	Standard ESU, Windows Server 2008	CVE-2023-35346	Remote Code Execution	Important	No	No	2
	Enterprise ESU	CVE-2023-33174	Information Disclosure	Important	No	No	2
		CVE-2023-35316	Information Disclosure	Important	No	No	2
		CVE-2023-35318	Denial of Service	Important	No	No	2
		ADV230001	Defense in Depth	None	No	Yes	0
		CVE-2023-35322	Remote Code Execution	Important	No	No	2
		CVE-2023-32038	Remote Code Execution	Important	No	No	2
		CVE-2023-35309	Remote Code Execution	Important	No	No	2
		CVE-2023-32035	Denial of Service	Important	No	No	2
		CVE-2023-35338	Denial of Service	Important	No	No	2
		CVE-2023-35351	Remote Code Execution	Important	No	No	2
		CVE-2023-35314	Denial of Service	Important	No	No	2
		CVE-2023-32033	Remote Code Execution	Important	No	No	2
		CVE-2023-32046	Elevation of Privilege	Important	No	Yes	0
		CVE-2023-35319	Denial of Service	Important	No	No	2
		CVE-2023-32057	Remote Code Execution	Critical	No	No	2
		CVE-2023-33173	Denial of Service	Important	No	No	2
		CVE-2023-35300	Remote Code Execution	Important	No	No	2
		CVE-2023-35350	Remote Code Execution	Important	No	No	2

		CVE-2023-35303	Remote Code Execution	Important	No	No	2
		CVE-2023-32045	Denial of Service	Important	No	No	2
		CVE-2023-33154	Elevation of Privilege	Important	No	No	2
		CVE-2023-33172	Denial of Service	Important	No	No	2
		CVE-2023-32034	Denial of Service	Important	No	No	2
		CVE-2023-33168	Denial of Service	Important	No	No	2
		CVE-2023-21526	Information Disclosure	Important	No	No	1
		CVE-2023-36874	Elevation of Privilege	Important	No	Yes	0
		CVE-2023-35345	Remote Code Execution	Important	No	No	2
		CVE-2023-32055	Elevation of Privilege	Important	No	No	2
		CVE-2023-35310	Remote Code Execution	Important	No	No	2
		CVE-2023-35297	Remote Code Execution	Critical	No	No	2
		CVE-2023-32043	Security Feature Bypass	Important	No	No	2
		CVE-2023-35321	Denial of Service	Important	No	No	2
		CVE-2023-33167	Denial of Service	Important	No	No	2
		CVE-2023-33166	Denial of Service	Important	No	No	2
		CVE-2023-35299	Elevation of Privilege	Important	No	No	2
		CVE-2023-32044	Denial of Service	Important	No	No	2
		CVE-2023-35328	Elevation of Privilege	Important	No	No	2
		CVE-2023-32050	Elevation of Privilege	Important	No	No	2

5028182	高危	July 11, 2023— KB5028182 (OS Build 22000.2176) – Microsoft Support for Windows 11 version 21H2, all editions	CVE-2023-35315	Remote Code Execution	Critical	No	No	2
			CVE-2023-33174	Information Disclosure	Important	No	No	2
			CVE-2023-35316	Information Disclosure	Important	No	No	2
			CVE-2023-35326	Information Disclosure	Important	No	No	2
			CVE-2023-32035	Denial of Service	Important	No	No	2
			CVE-2023-35343	Remote Code Execution	Important	No	No	2
			CVE-2023-35302	Remote Code Execution	Important	No	No	2
			CVE-2023-35337	Elevation of Privilege	Important	No	No	2
			CVE-2023-35308	Security Feature Bypass	Important	No	No	2
			CVE-2023-35296	Information Disclosure	Important	No	No	2
			CVE-2023-32041	Information Disclosure	Important	No	No	2
			CVE-2023-35358	Elevation of Privilege	Important	No	No	2
			CVE-2023-35341	Information Disclosure	Important	No	No	2
			CVE-2023-33172	Denial of Service	Important	No	No	2
			CVE-2023-32034	Denial of Service	Important	No	No	2
			CVE-2023-33168	Denial of Service	Important	No	No	2
			CVE-2023-35320	Elevation of Privilege	Important	No	No	2
			CVE-2023-32042	Information Disclosure	Important	No	No	2
			CVE-2023-35365	Remote Code Execution	Critical	No	No	2
			CVE-2023-35342	Elevation of Privilege	Important	No	No	2

			CVE-2023-32085	Information Disclosure	Important	No	No	2
			CVE-2023-32049	Security Feature Bypass	Important	No	Yes	0
			CVE-2023-21756	Elevation of Privilege	Important	No	No	2
			CVE-2023-35323	Remote Code Execution	Important	No	No	2
			CVE-2023-35313	Remote Code Execution	Important	No	No	2
			CVE-2023-35325	Information Disclosure	Important	No	No	2
			CVE-2023-35306	Information Disclosure	Important	No	No	2
			CVE-2023-35324	Information Disclosure	Important	No	No	2
			CVE-2023-35356	Elevation of Privilege	Important	No	No	2
			CVE-2023-35314	Denial of Service	Important	No	No	2
			CVE-2023-35319	Denial of Service	Important	No	No	2
			CVE-2023-32040	Information Disclosure	Important	No	No	2
			CVE-2023-32057	Remote Code Execution	Critical	No	No	2
			CVE-2023-35360	Elevation of Privilege	Important	No	No	2
			CVE-2023-32045	Denial of Service	Important	No	No	2
			CVE-2023-33173	Denial of Service	Important	No	No	2
			CVE-2023-35303	Remote Code Execution	Important	No	No	2
			CVE-2023-35329	Denial of Service	Important	No	No	2
			CVE-2023-35353	Elevation of Privilege	Important	No	No	2
			CVE-2023-36874	Elevation of Privilege	Important	No	Yes	0

		CVE-2023-35297	Remote Code Execution	Critical	No	No	2
		CVE-2023-33166	Denial of Service	Important	No	No	2
		CVE-2023-32056	Elevation of Privilege	Important	No	No	2
		CVE-2023-35299	Elevation of Privilege	Important	No	No	2
		CVE-2023-32044	Denial of Service	Important	No	No	2
		CVE-2023-32053	Elevation of Privilege	Important	No	No	2
		CVE-2023-35340	Elevation of Privilege	Important	No	No	2
		CVE-2023-35367	Remote Code Execution	Critical	No	No	2
		CVE-2023-32039	Information Disclosure	Important	No	No	2
		CVE-2023-32037	Information Disclosure	Important	No	No	2
		CVE-2023-35318	Denial of Service	Important	No	No	2
		CVE-2023-35312	Elevation of Privilege	Important	No	No	1
		CVE-2023-32084	Denial of Service	Important	No	No	2
		CVE-2023-32046	Elevation of Privilege	Important	No	Yes	0
		CVE-2023-35364	Elevation of Privilege	Important	No	No	2
		CVE-2023-35300	Remote Code Execution	Important	No	No	2
		CVE-2023-33155	Elevation of Privilege	Important	No	No	2
		ADV230002	Security Feature Bypass	Important	No	No	2
		CVE-2023-21526	Information Disclosure	Important	No	No	1
		CVE-2023-32055	Elevation of Privilege	Important	No	No	2

			CVE-2023-32043	Security Feature Bypass	Important	No	No	2
			CVE-2023-35366	Remote Code Execution	Critical	No	No	2
			CVE-2023-33164	Denial of Service	Important	No	No	2
			CVE-2023-33169	Denial of Service	Important	No	No	2
			CVE-2023-35305	Elevation of Privilege	Important	No	No	2
			CVE-2023-35336	Security Feature Bypass	Important	No	No	2
			CVE-2023-35347	Elevation of Privilege	Important	No	No	2
			CVE-2023-35330	Denial of Service	Important	No	No	2
			CVE-2023-36871	Security Feature Bypass	Important	No	No	1
			CVE-2023-35339	Denial of Service	Important	No	No	2
			CVE-2023-35357	Elevation of Privilege	Important	No	No	2
			CVE-2023-35309	Remote Code Execution	Important	No	No	2
			CVE-2023-32038	Remote Code Execution	Important	No	No	2
			CVE-2023-35338	Denial of Service	Important	No	No	2
			CVE-2023-35363	Elevation of Privilege	Important	No	No	2
			CVE-2023-35298	Denial of Service	Important	No	No	2
			CVE-2023-35304	Elevation of Privilege	Important	No	No	2
			CVE-2023-33154	Elevation of Privilege	Important	No	No	2
			CVE-2023-35332	Security Feature Bypass	Important	No	No	2

			CVE-2023-33167	Denial of Service	Important	No	No	2
			CVE-2023-35362	Elevation of Privilege	Important	No	No	2
			CVE-2023-32054	Elevation of Privilege	Important	No	No	2
			CVE-2023-35328	Elevation of Privilege	Important	No	No	2
			ADV230001	Defense in Depth	None	No	Yes	0
			CVE-2023-35361	Elevation of Privilege	Important	No	No	2
5028223	高危	July 11, 2023—KB5028223 (Security-only update) – Microsoft Support for Windows Server 2012 R2, Windows Embedded 8.1 Industry Enterprise, Windows Embedded 8.1 Industry Pro	CVE-2023-35366	Remote Code Execution	Critical	No	No	2
			CVE-2023-33164	Denial of Service	Important	No	No	2
			CVE-2023-35365	Remote Code Execution	Critical	No	No	2
			CVE-2023-32053	Elevation of Privilege	Important	No	No	2
			CVE-2023-33169	Denial of Service	Important	No	No	2
			CVE-2023-35340	Elevation of Privilege	Important	No	No	2
			CVE-2023-35344	Remote Code Execution	Important	No	No	2
			CVE-2023-35336	Security Feature Bypass	Important	No	No	2
			CVE-2023-35367	Remote Code Execution	Critical	No	No	2
			CVE-2023-35331	Denial of Service	Important	No	No	2
			CVE-2023-35330	Denial of Service	Important	No	No	2
			CVE-2023-32039	Information Disclosure	Important	No	No	2
			CVE-2023-33163	Remote Code Execution	Important	No	No	2
			CVE-2023-35342	Elevation of Privilege	Important	No	No	2

		CVE-2023-32085	Information Disclosure	Important	No	No	2
		CVE-2023-35346	Remote Code Execution	Important	No	No	2
		CVE-2023-33174	Information Disclosure	Important	No	No	2
		CVE-2023-35316	Information Disclosure	Important	No	No	2
		CVE-2023-35318	Denial of Service	Important	No	No	2
		CVE-2023-21756	Elevation of Privilege	Important	No	No	2
		CVE-2023-35352	Security Feature Bypass	Critical	No	No	1
		ADV230001	Defense in Depth	None	No	Yes	0
		CVE-2023-35322	Remote Code Execution	Important	No	No	2
		CVE-2023-35312	Elevation of Privilege	Important	No	No	1
		CVE-2023-32038	Remote Code Execution	Important	No	No	2
		CVE-2023-35309	Remote Code Execution	Important	No	No	2
		CVE-2023-35325	Information Disclosure	Important	No	No	2
		CVE-2023-32035	Denial of Service	Important	No	No	2
		CVE-2023-35317	Elevation of Privilege	Important	No	No	2
		CVE-2023-35302	Remote Code Execution	Important	No	No	2
		CVE-2023-35338	Denial of Service	Important	No	No	2
		CVE-2023-35306	Information Disclosure	Important	No	No	2
		CVE-2023-35308	Security Feature Bypass	Important	No	No	2

			CVE-2023-35351	Remote Code Execution	Important	No	No	2
			CVE-2023-35324	Information Disclosure	Important	No	No	2
			CVE-2023-35296	Information Disclosure	Important	No	No	2
			CVE-2023-35314	Denial of Service	Important	No	No	2
			CVE-2023-32033	Remote Code Execution	Important	No	No	2
			CVE-2023-32046	Elevation of Privilege	Important	No	Yes	0
			CVE-2023-35319	Denial of Service	Important	No	No	2
			CVE-2023-32040	Information Disclosure	Important	No	No	2
			CVE-2023-32057	Remote Code Execution	Critical	No	No	2
			CVE-2023-35360	Elevation of Privilege	Important	No	No	2
			CVE-2023-35300	Remote Code Execution	Important	No	No	2
			CVE-2023-35350	Remote Code Execution	Important	No	No	2
			CVE-2023-35303	Remote Code Execution	Important	No	No	2
			CVE-2023-32045	Denial of Service	Important	No	No	2
			CVE-2023-35341	Information Disclosure	Important	No	No	2
			CVE-2023-33154	Elevation of Privilege	Important	No	No	2
			CVE-2023-33173	Denial of Service	Important	No	No	2
			CVE-2023-33172	Denial of Service	Important	No	No	2
			CVE-2023-32034	Denial of Service	Important	No	No	2
			CVE-2023-35329	Denial of Service	Important	No	No	2

			ADV230002	Security Feature Bypass	Important	No	No	2
			CVE-2023-33168	Denial of Service	Important	No	No	2
			CVE-2023-21526	Information Disclosure	Important	No	No	1
			CVE-2023-36874	Elevation of Privilege	Important	No	Yes	0
			CVE-2023-35345	Remote Code Execution	Important	No	No	2
			CVE-2023-32055	Elevation of Privilege	Important	No	No	2
			CVE-2023-35310	Remote Code Execution	Important	No	No	2
			CVE-2023-35332	Security Feature Bypass	Important	No	No	2
			CVE-2023-35297	Remote Code Execution	Critical	No	No	2
			CVE-2023-35321	Denial of Service	Important	No	No	2
			CVE-2023-32043	Security Feature Bypass	Important	No	No	2
			CVE-2023-33167	Denial of Service	Important	No	No	2
			CVE-2023-33166	Denial of Service	Important	No	No	2
			CVE-2023-35299	Elevation of Privilege	Important	No	No	2
			CVE-2023-32044	Denial of Service	Important	No	No	2
			CVE-2023-35328	Elevation of Privilege	Important	No	No	2
			CVE-2023-32042	Information Disclosure	Important	No	No	2
			CVE-2023-35361	Elevation of Privilege	Important	No	No	2
5028224	高危	July 11, 2023—	CVE-2023-35366	Remote Code Execution	Critical	No	No	2

KB5028224 (Security -only update) - Microsoft Support for Windows Server 2008 R2 Enterpris e ESU, Windo ws Server 2008 R2 Standard ESU, Windo ws Server 2008 R2 Datacente r ESU, Windo ws Embedded Standard 7 ESU, Windo ws Embedded POSReady 7 ESU	CVE-2023-33164	Denial of Service	Important	No	No	2
	CVE-2023-35365	Remote Code Execution	Critical	No	No	2
	CVE-2023-32053	Elevation of Privilege	Important	No	No	2
	CVE-2023-33169	Denial of Service	Important	No	No	2
	CVE-2023-35340	Elevation of Privilege	Important	No	No	2
	CVE-2023-35344	Remote Code Execution	Important	No	No	2
	CVE-2023-35367	Remote Code Execution	Critical	No	No	2
	CVE-2023-35330	Denial of Service	Important	No	No	2
	CVE-2023-33163	Remote Code Execution	Important	No	No	2
	CVE-2023-32042	Information Disclosure	Important	No	No	2
	CVE-2023-35342	Elevation of Privilege	Important	No	No	2
	CVE-2023-35346	Remote Code Execution	Important	No	No	2
	CVE-2023-33174	Information Disclosure	Important	No	No	2
	CVE-2023-35316	Information Disclosure	Important	No	No	2
	CVE-2023-35318	Denial of Service	Important	No	No	2
	ADV230001	Defense in Depth	None	No	Yes	0
	CVE-2023-35322	Remote Code Execution	Important	No	No	2
CVE-2023-35312	Elevation of Privilege	Important	No	No	1	
CVE-2023-32038	Remote Code Execution	Important	No	No	2	
CVE-2023-35309	Remote Code Execution	Important	No	No	2	

			CVE-2023-32035	Denial of Service	Important	No	No	2
			CVE-2023-35338	Denial of Service	Important	No	No	2
			CVE-2023-35351	Remote Code Execution	Important	No	No	2
			CVE-2023-35314	Denial of Service	Important	No	No	2
			CVE-2023-35299	Elevation of Privilege	Important	No	No	2
			CVE-2023-32033	Remote Code Execution	Important	No	No	2
			CVE-2023-32046	Elevation of Privilege	Important	No	Yes	0
			CVE-2023-35319	Denial of Service	Important	No	No	2
			CVE-2023-32057	Remote Code Execution	Critical	No	No	2
			CVE-2023-33173	Denial of Service	Important	No	No	2
			CVE-2023-35300	Remote Code Execution	Important	No	No	2
			CVE-2023-35350	Remote Code Execution	Important	No	No	2
			CVE-2023-35303	Remote Code Execution	Important	No	No	2
			CVE-2023-32045	Denial of Service	Important	No	No	2
			CVE-2023-35341	Information Disclosure	Important	No	No	2
			CVE-2023-33154	Elevation of Privilege	Important	No	No	2
			CVE-2023-33172	Denial of Service	Important	No	No	2
			CVE-2023-32034	Denial of Service	Important	No	No	2
			CVE-2023-33168	Denial of Service	Important	No	No	2
			CVE-2023-21526	Information Disclosure	Important	No	No	1

			CVE-2023-35345	Remote Code Execution	Important	No	No	2
			CVE-2023-32055	Elevation of Privilege	Important	No	No	2
			CVE-2023-35310	Remote Code Execution	Important	No	No	2
			CVE-2023-35332	Security Feature Bypass	Important	No	No	2
			CVE-2023-35297	Remote Code Execution	Critical	No	No	2
			CVE-2023-35321	Denial of Service	Important	No	No	2
			CVE-2023-32043	Security Feature Bypass	Important	No	No	2
			CVE-2023-33167	Denial of Service	Important	No	No	2
			CVE-2023-33166	Denial of Service	Important	No	No	2
			CVE-2023-32054	Elevation of Privilege	Important	No	No	2
			CVE-2023-32044	Denial of Service	Important	No	No	2
			CVE-2023-35328	Elevation of Privilege	Important	No	No	2
			CVE-2023-32050	Elevation of Privilege	Important	No	No	2
5028169	高危	July 11, 2023— KB5028169 (OS Build 14393.608 5) – Microsoft Support for Windows 10, version	CVE-2023-35344	Remote Code Execution	Important	No	No	2
			CVE-2023-33163	Remote Code Execution	Important	No	No	2
			CVE-2023-33174	Information Disclosure	Important	No	No	2
			CVE-2023-35316	Information Disclosure	Important	No	No	2
			CVE-2023-32035	Denial of Service	Important	No	No	2
			CVE-2023-35302	Remote Code Execution	Important	No	No	2

	1607, all editions, Windows Server 2016, all editions	CVE-2023-35308	Security Feature Bypass	Important	No	No	2
		CVE-2023-35296	Information Disclosure	Important	No	No	2
		CVE-2023-32041	Information Disclosure	Important	No	No	2
		CVE-2023-35350	Remote Code Execution	Important	No	No	2
		CVE-2023-35358	Elevation of Privilege	Important	No	No	2
		CVE-2023-35341	Information Disclosure	Important	No	No	2
		CVE-2023-33172	Denial of Service	Important	No	No	2
		CVE-2023-32034	Denial of Service	Important	No	No	2
		CVE-2023-33168	Denial of Service	Important	No	No	2
		CVE-2023-35345	Remote Code Execution	Important	No	No	2
		CVE-2023-35320	Elevation of Privilege	Important	No	No	2
		CVE-2023-32042	Information Disclosure	Important	No	No	2
		CVE-2023-35352	Security Feature Bypass	Critical	No	No	1
		CVE-2023-35365	Remote Code Execution	Critical	No	No	2
		CVE-2023-35342	Elevation of Privilege	Important	No	No	2
		CVE-2023-32085	Information Disclosure	Important	No	No	2
		CVE-2023-32049	Security Feature Bypass	Important	No	Yes	0
		CVE-2023-21756	Elevation of Privilege	Important	No	No	2
		CVE-2023-35313	Remote Code Execution	Important	No	No	2

		CVE-2023-35325	Information Disclosure	Important	No	No	2
		CVE-2023-35306	Information Disclosure	Important	No	No	2
		CVE-2023-32083	Information Disclosure	Important	No	No	2
		CVE-2023-35356	Elevation of Privilege	Important	No	No	2
		CVE-2023-35324	Information Disclosure	Important	No	No	2
		CVE-2023-35314	Denial of Service	Important	No	No	2
		CVE-2023-35319	Denial of Service	Important	No	No	2
		CVE-2023-32040	Information Disclosure	Important	No	No	2
		CVE-2023-35360	Elevation of Privilege	Important	No	No	2
		CVE-2023-32057	Remote Code Execution	Critical	No	No	2
		CVE-2023-32045	Denial of Service	Important	No	No	2
		CVE-2023-33173	Denial of Service	Important	No	No	2
		CVE-2023-35303	Remote Code Execution	Important	No	No	2
		CVE-2023-35329	Denial of Service	Important	No	No	2
		CVE-2023-35353	Elevation of Privilege	Important	No	No	2
		CVE-2023-36874	Elevation of Privilege	Important	No	Yes	0
		CVE-2023-35297	Remote Code Execution	Critical	No	No	2
		CVE-2023-35310	Remote Code Execution	Important	No	No	2
		CVE-2023-33166	Denial of Service	Important	No	No	2
		CVE-2023-35299	Elevation of Privilege	Important	No	No	2

			CVE-2023-32044	Denial of Service	Important	No	No	2
			CVE-2023-32053	Elevation of Privilege	Important	No	No	2
			CVE-2023-35340	Elevation of Privilege	Important	No	No	2
			CVE-2023-35367	Remote Code Execution	Critical	No	No	2
			CVE-2023-32039	Information Disclosure	Important	No	No	2
			CVE-2023-35318	Denial of Service	Important	No	No	2
			CVE-2023-35312	Elevation of Privilege	Important	No	No	1
			CVE-2023-35348	Security Feature Bypass	Important	No	No	2
			CVE-2023-35317	Elevation of Privilege	Important	No	No	2
			CVE-2023-32046	Elevation of Privilege	Important	No	Yes	0
			CVE-2023-35300	Remote Code Execution	Important	No	No	2
			ADV230002	Security Feature Bypass	Important	No	No	2
			CVE-2023-21526	Information Disclosure	Important	No	No	1
			CVE-2023-32055	Elevation of Privilege	Important	No	No	2
			CVE-2023-32043	Security Feature Bypass	Important	No	No	2
			CVE-2023-35366	Remote Code Execution	Critical	No	No	2
			CVE-2023-33164	Denial of Service	Important	No	No	2
			CVE-2023-33169	Denial of Service	Important	No	No	2
			CVE-2023-35305	Elevation of Privilege	Important	No	No	2

			CVE-2023-35336	Security Feature Bypass	Important	No	No	2
			CVE-2023-35331	Denial of Service	Important	No	No	2
			CVE-2023-35330	Denial of Service	Important	No	No	2
			CVE-2023-36871	Security Feature Bypass	Important	No	No	1
			CVE-2023-35339	Denial of Service	Important	No	No	2
			CVE-2023-35346	Remote Code Execution	Important	No	No	2
			CVE-2023-35357	Elevation of Privilege	Important	No	No	2
			CVE-2023-35322	Remote Code Execution	Important	No	No	2
			CVE-2023-32038	Remote Code Execution	Important	No	No	2
			CVE-2023-35309	Remote Code Execution	Important	No	No	2
			CVE-2023-35338	Denial of Service	Important	No	No	2
			CVE-2023-35351	Remote Code Execution	Important	No	No	2
			CVE-2023-32033	Remote Code Execution	Important	No	No	2
			CVE-2023-35304	Elevation of Privilege	Important	No	No	2
			CVE-2023-33154	Elevation of Privilege	Important	No	No	2
			CVE-2023-35332	Security Feature Bypass	Important	No	No	2
			CVE-2023-33167	Denial of Service	Important	No	No	2
			CVE-2023-35321	Denial of Service	Important	No	No	2
			CVE-2023-35362	Elevation of Privilege	Important	No	No	2

			CVE-2023-32054	Elevation of Privilege	Important	No	No	2
			CVE-2023-35328	Elevation of Privilege	Important	No	No	2
			ADV230001	Defense in Depth	None	No	Yes	0
			CVE-2023-35361	Elevation of Privilege	Important	No	No	2
5028240	高危	July 11, 2023—KB5028240 (Monthly Rollup) – Microsoft Support for Windows Server 2008 R2 Enterprise ESU, Windows Server 2008 R2 Standard ESU, Windows Server 2008 R2 Datacenter ESU, Windows Embedded Standard 7 ESU, Windows Embedded POSReady 7 ESU	CVE-2023-35366	Remote Code Execution	Critical	No	No	2
			CVE-2023-33164	Denial of Service	Important	No	No	2
			CVE-2023-35365	Remote Code Execution	Critical	No	No	2
			CVE-2023-32053	Elevation of Privilege	Important	No	No	2
			CVE-2023-33169	Denial of Service	Important	No	No	2
			CVE-2023-35340	Elevation of Privilege	Important	No	No	2
			CVE-2023-35344	Remote Code Execution	Important	No	No	2
			CVE-2023-35367	Remote Code Execution	Critical	No	No	2
			CVE-2023-35330	Denial of Service	Important	No	No	2
			CVE-2023-33163	Remote Code Execution	Important	No	No	2
			CVE-2023-32042	Information Disclosure	Important	No	No	2
			CVE-2023-35342	Elevation of Privilege	Important	No	No	2
			CVE-2023-35346	Remote Code Execution	Important	No	No	2
			CVE-2023-33174	Information Disclosure	Important	No	No	2
			CVE-2023-35316	Information Disclosure	Important	No	No	2
			CVE-2023-35318	Denial of Service	Important	No	No	2

		ADV230001	Defense in Depth	None	No	Yes	0
		CVE-2023-35322	Remote Code Execution	Important	No	No	2
		CVE-2023-35312	Elevation of Privilege	Important	No	No	1
		CVE-2023-32038	Remote Code Execution	Important	No	No	2
		CVE-2023-35309	Remote Code Execution	Important	No	No	2
		CVE-2023-32035	Denial of Service	Important	No	No	2
		CVE-2023-35338	Denial of Service	Important	No	No	2
		CVE-2023-35351	Remote Code Execution	Important	No	No	2
		CVE-2023-35314	Denial of Service	Important	No	No	2
		CVE-2023-35299	Elevation of Privilege	Important	No	No	2
		CVE-2023-32033	Remote Code Execution	Important	No	No	2
		CVE-2023-32046	Elevation of Privilege	Important	No	Yes	0
		CVE-2023-35319	Denial of Service	Important	No	No	2
		CVE-2023-32057	Remote Code Execution	Critical	No	No	2
		CVE-2023-33173	Denial of Service	Important	No	No	2
		CVE-2023-35300	Remote Code Execution	Important	No	No	2
		CVE-2023-35350	Remote Code Execution	Important	No	No	2
		CVE-2023-35303	Remote Code Execution	Important	No	No	2
		CVE-2023-32045	Denial of Service	Important	No	No	2
		CVE-2023-35341	Information Disclosure	Important	No	No	2

			CVE-2023-33154	Elevation of Privilege	Important	No	No	2
			CVE-2023-33172	Denial of Service	Important	No	No	2
			CVE-2023-32034	Denial of Service	Important	No	No	2
			CVE-2023-33168	Denial of Service	Important	No	No	2
			CVE-2023-21526	Information Disclosure	Important	No	No	1
			CVE-2023-36874	Elevation of Privilege	Important	No	Yes	0
			CVE-2023-35345	Remote Code Execution	Important	No	No	2
			CVE-2023-32055	Elevation of Privilege	Important	No	No	2
			CVE-2023-35310	Remote Code Execution	Important	No	No	2
			CVE-2023-35332	Security Feature Bypass	Important	No	No	2
			CVE-2023-35297	Remote Code Execution	Critical	No	No	2
			CVE-2023-35321	Denial of Service	Important	No	No	2
			CVE-2023-32043	Security Feature Bypass	Important	No	No	2
			CVE-2023-33167	Denial of Service	Important	No	No	2
			CVE-2023-33166	Denial of Service	Important	No	No	2
			CVE-2023-32054	Elevation of Privilege	Important	No	No	2
			CVE-2023-32044	Denial of Service	Important	No	No	2
			CVE-2023-35328	Elevation of Privilege	Important	No	No	2
			CVE-2023-32050	Elevation of Privilege	Important	No	No	2

5028185	高危	July 11, 2023— KB5028185 (OS Build 22621.1992) - Microsoft Support for Windows 11 version 22H2, all editions	CVE-2023-35315	Remote Code Execution	Critical	No	No	2
			CVE-2023-33174	Information Disclosure	Important	No	No	2
			CVE-2023-35316	Information Disclosure	Important	No	No	2
			CVE-2023-35326	Information Disclosure	Important	No	No	2
			CVE-2023-32035	Denial of Service	Important	No	No	2
			CVE-2023-35343	Remote Code Execution	Important	No	No	2
			CVE-2023-35302	Remote Code Execution	Important	No	No	2
			CVE-2023-35337	Elevation of Privilege	Important	No	No	2
			CVE-2023-35308	Security Feature Bypass	Important	No	No	2
			CVE-2023-35296	Information Disclosure	Important	No	No	2
			CVE-2023-32041	Information Disclosure	Important	No	No	2
			CVE-2023-35358	Elevation of Privilege	Important	No	No	2
			CVE-2023-35341	Information Disclosure	Important	No	No	2
			CVE-2023-33172	Denial of Service	Important	No	No	2
			CVE-2023-32034	Denial of Service	Important	No	No	2
			CVE-2023-33168	Denial of Service	Important	No	No	2
			CVE-2023-35320	Elevation of Privilege	Important	No	No	2
			CVE-2023-32042	Information Disclosure	Important	No	No	2
			CVE-2023-35365	Remote Code Execution	Critical	No	No	2
			CVE-2023-35342	Elevation of Privilege	Important	No	No	2

			CVE-2023-32085	Information Disclosure	Important	No	No	2
			CVE-2023-32049	Security Feature Bypass	Important	No	Yes	0
			CVE-2023-21756	Elevation of Privilege	Important	No	No	2
			CVE-2023-35313	Remote Code Execution	Important	No	No	2
			CVE-2023-35325	Information Disclosure	Important	No	No	2
			CVE-2023-35306	Information Disclosure	Important	No	No	2
			CVE-2023-35324	Information Disclosure	Important	No	No	2
			CVE-2023-35356	Elevation of Privilege	Important	No	No	2
			CVE-2023-35314	Denial of Service	Important	No	No	2
			CVE-2023-35319	Denial of Service	Important	No	No	2
			CVE-2023-32040	Information Disclosure	Important	No	No	2
			CVE-2023-32057	Remote Code Execution	Critical	No	No	2
			CVE-2023-35360	Elevation of Privilege	Important	No	No	2
			CVE-2023-32045	Denial of Service	Important	No	No	2
			CVE-2023-33173	Denial of Service	Important	No	No	2
			CVE-2023-35303	Remote Code Execution	Important	No	No	2
			CVE-2023-35329	Denial of Service	Important	No	No	2
			CVE-2023-35353	Elevation of Privilege	Important	No	No	2
			CVE-2023-36874	Elevation of Privilege	Important	No	Yes	0
			CVE-2023-35297	Remote Code Execution	Critical	No	No	2

			CVE-2023-33166	Denial of Service	Important	No	No	2
			CVE-2023-32056	Elevation of Privilege	Important	No	No	2
			CVE-2023-35299	Elevation of Privilege	Important	No	No	2
			CVE-2023-32044	Denial of Service	Important	No	No	2
			CVE-2023-32053	Elevation of Privilege	Important	No	No	2
			CVE-2023-35340	Elevation of Privilege	Important	No	No	2
			CVE-2023-35367	Remote Code Execution	Critical	No	No	2
			CVE-2023-32039	Information Disclosure	Important	No	No	2
			CVE-2023-32037	Information Disclosure	Important	No	No	2
			CVE-2023-35318	Denial of Service	Important	No	No	2
			CVE-2023-35312	Elevation of Privilege	Important	No	No	1
			CVE-2023-32084	Denial of Service	Important	No	No	2
			CVE-2023-32046	Elevation of Privilege	Important	No	Yes	0
			CVE-2023-35364	Elevation of Privilege	Important	No	No	2
			CVE-2023-35300	Remote Code Execution	Important	No	No	2
			CVE-2023-33155	Elevation of Privilege	Important	No	No	2
			ADV230002	Security Feature Bypass	Important	No	No	2
			CVE-2023-21526	Information Disclosure	Important	No	No	1
			CVE-2023-32055	Elevation of Privilege	Important	No	No	2

			CVE-2023-32043	Security Feature Bypass	Important	No	No	2
			CVE-2023-35366	Remote Code Execution	Critical	No	No	2
			CVE-2023-33164	Denial of Service	Important	No	No	2
			CVE-2023-33169	Denial of Service	Important	No	No	2
			CVE-2023-35305	Elevation of Privilege	Important	No	No	2
			CVE-2023-35336	Security Feature Bypass	Important	No	No	2
			CVE-2023-35347	Elevation of Privilege	Important	No	No	2
			CVE-2023-35330	Denial of Service	Important	No	No	2
			CVE-2023-36871	Security Feature Bypass	Important	No	No	1
			CVE-2023-35339	Denial of Service	Important	No	No	2
			CVE-2023-35357	Elevation of Privilege	Important	No	No	2
			CVE-2023-35309	Remote Code Execution	Important	No	No	2
			CVE-2023-32038	Remote Code Execution	Important	No	No	2
			CVE-2023-35338	Denial of Service	Important	No	No	2
			CVE-2023-35363	Elevation of Privilege	Important	No	No	2
			CVE-2023-35298	Denial of Service	Important	No	No	2
			CVE-2023-35304	Elevation of Privilege	Important	No	No	2
			CVE-2023-33154	Elevation of Privilege	Important	No	No	2
			CVE-2023-35332	Security Feature Bypass	Important	No	No	2

			CVE-2023-33167	Denial of Service	Important	No	No	2
			CVE-2023-35362	Elevation of Privilege	Important	No	No	2
			CVE-2023-32054	Elevation of Privilege	Important	No	No	2
			CVE-2023-35328	Elevation of Privilege	Important	No	No	2
			ADV230001	Defense in Depth	None	No	Yes	0
			CVE-2023-35361	Elevation of Privilege	Important	No	No	2
5028186	高危	July 11, 2023— KB5028186 (OS Build 10240.20048) – Microsoft Support for Windows 10	CVE-2023-35366	Remote Code Execution	Critical	No	No	2
			CVE-2023-33164	Denial of Service	Important	No	No	2
			CVE-2023-35365	Remote Code Execution	Critical	No	No	2
			CVE-2023-32053	Elevation of Privilege	Important	No	No	2
			CVE-2023-33169	Denial of Service	Important	No	No	2
			CVE-2023-35340	Elevation of Privilege	Important	No	No	2
			CVE-2023-35336	Security Feature Bypass	Important	No	No	2
			CVE-2023-35367	Remote Code Execution	Critical	No	No	2
			CVE-2023-35330	Denial of Service	Important	No	No	2
			CVE-2023-32039	Information Disclosure	Important	No	No	2
			CVE-2023-35342	Elevation of Privilege	Important	No	No	2
			CVE-2023-36871	Security Feature Bypass	Important	No	No	1
			CVE-2023-32085	Information Disclosure	Important	No	No	2

		CVE-2023-35339	Denial of Service	Important	No	No	2
		CVE-2023-33174	Information Disclosure	Important	No	No	2
		CVE-2023-35316	Information Disclosure	Important	No	No	2
		CVE-2023-35318	Denial of Service	Important	No	No	2
		CVE-2023-21756	Elevation of Privilege	Important	No	No	2
		ADV230001	Defense in Depth	None	No	Yes	0
		CVE-2023-35313	Remote Code Execution	Important	No	No	2
		CVE-2023-35312	Elevation of Privilege	Important	No	No	1
		CVE-2023-35309	Remote Code Execution	Important	No	No	2
		CVE-2023-32038	Remote Code Execution	Important	No	No	2
		CVE-2023-35325	Information Disclosure	Important	No	No	2
		CVE-2023-32035	Denial of Service	Important	No	No	2
		CVE-2023-35302	Remote Code Execution	Important	No	No	2
		CVE-2023-35338	Denial of Service	Important	No	No	2
		CVE-2023-35306	Information Disclosure	Important	No	No	2
		CVE-2023-35308	Security Feature Bypass	Important	No	No	2
		CVE-2023-35324	Information Disclosure	Important	No	No	2
		CVE-2023-35296	Information Disclosure	Important	No	No	2
		CVE-2023-35314	Denial of Service	Important	No	No	2
		CVE-2023-35299	Elevation of Privilege	Important	No	No	2

			CVE-2023-32046	Elevation of Privilege	Important	No	Yes	0
			CVE-2023-35319	Denial of Service	Important	No	No	2
			CVE-2023-32040	Information Disclosure	Important	No	No	2
			CVE-2023-35360	Elevation of Privilege	Important	No	No	2
			CVE-2023-32057	Remote Code Execution	Critical	No	No	2
			CVE-2023-35300	Remote Code Execution	Important	No	No	2
			CVE-2023-32045	Denial of Service	Important	No	No	2
			CVE-2023-35303	Remote Code Execution	Important	No	No	2
			CVE-2023-33173	Denial of Service	Important	No	No	2
			CVE-2023-35341	Information Disclosure	Important	No	No	2
			CVE-2023-33154	Elevation of Privilege	Important	No	No	2
			CVE-2023-33172	Denial of Service	Important	No	No	2
			CVE-2023-32034	Denial of Service	Important	No	No	2
			CVE-2023-35329	Denial of Service	Important	No	No	2
			ADV230002	Security Feature Bypass	Important	No	No	2
			CVE-2023-33168	Denial of Service	Important	No	No	2
			CVE-2023-21526	Information Disclosure	Important	No	No	1
			CVE-2023-36874	Elevation of Privilege	Important	No	Yes	0
			CVE-2023-35332	Security Feature Bypass	Important	No	No	2

			CVE-2023-32055	Elevation of Privilege	Important	No	No	2
			CVE-2023-35297	Remote Code Execution	Critical	No	No	2
			CVE-2023-32043	Security Feature Bypass	Important	No	No	2
			CVE-2023-33167	Denial of Service	Important	No	No	2
			CVE-2023-33166	Denial of Service	Important	No	No	2
			CVE-2023-35362	Elevation of Privilege	Important	No	No	2
			CVE-2023-32054	Elevation of Privilege	Important	No	No	2
			CVE-2023-32044	Denial of Service	Important	No	No	2
			CVE-2023-35328	Elevation of Privilege	Important	No	No	2
			CVE-2023-32042	Information Disclosure	Important	No	No	2
			CVE-2023-35361	Elevation of Privilege	Important	No	No	2
5028226	高危	July 11, 2023—KB5028226 (Security-only update) – Microsoft Support for Windows Server 2008 Datacenter ESU, Windows Server 2008 Standard	CVE-2023-35366	Remote Code Execution	Critical	No	No	2
			CVE-2023-33164	Denial of Service	Important	No	No	2
			CVE-2023-35365	Remote Code Execution	Critical	No	No	2
			CVE-2023-33169	Denial of Service	Important	No	No	2
			CVE-2023-35340	Elevation of Privilege	Important	No	No	2
			CVE-2023-35344	Remote Code Execution	Important	No	No	2
			CVE-2023-35367	Remote Code Execution	Critical	No	No	2
			CVE-2023-32042	Information Disclosure	Important	No	No	2
			CVE-2023-35346	Remote Code Execution	Important	No	No	2

ESU, Windows Server 2008 Enterprise ESU	CVE-2023-33174	Information Disclosure	Important	No	No	2
	CVE-2023-35316	Information Disclosure	Important	No	No	2
	CVE-2023-35318	Denial of Service	Important	No	No	2
	ADV230001	Defense in Depth	None	No	Yes	0
	CVE-2023-35322	Remote Code Execution	Important	No	No	2
	CVE-2023-32038	Remote Code Execution	Important	No	No	2
	CVE-2023-35309	Remote Code Execution	Important	No	No	2
	CVE-2023-32035	Denial of Service	Important	No	No	2
	CVE-2023-35338	Denial of Service	Important	No	No	2
	CVE-2023-35351	Remote Code Execution	Important	No	No	2
	CVE-2023-35314	Denial of Service	Important	No	No	2
	CVE-2023-32033	Remote Code Execution	Important	No	No	2
	CVE-2023-32046	Elevation of Privilege	Important	No	Yes	0
	CVE-2023-35319	Denial of Service	Important	No	No	2
	CVE-2023-32057	Remote Code Execution	Critical	No	No	2
	CVE-2023-33173	Denial of Service	Important	No	No	2
	CVE-2023-35300	Remote Code Execution	Important	No	No	2
	CVE-2023-35350	Remote Code Execution	Important	No	No	2
	CVE-2023-35303	Remote Code Execution	Important	No	No	2
	CVE-2023-32045	Denial of Service	Important	No	No	2

			CVE-2023-33154	Elevation of Privilege	Important	No	No	2
			CVE-2023-33172	Denial of Service	Important	No	No	2
			CVE-2023-32034	Denial of Service	Important	No	No	2
			CVE-2023-33168	Denial of Service	Important	No	No	2
			CVE-2023-21526	Information Disclosure	Important	No	No	1
			CVE-2023-36874	Elevation of Privilege	Important	No	Yes	0
			CVE-2023-35345	Remote Code Execution	Important	No	No	2
			CVE-2023-32055	Elevation of Privilege	Important	No	No	2
			CVE-2023-35310	Remote Code Execution	Important	No	No	2
			CVE-2023-35297	Remote Code Execution	Critical	No	No	2
			CVE-2023-32043	Security Feature Bypass	Important	No	No	2
			CVE-2023-35321	Denial of Service	Important	No	No	2
			CVE-2023-33167	Denial of Service	Important	No	No	2
			CVE-2023-33166	Denial of Service	Important	No	No	2
			CVE-2023-35299	Elevation of Privilege	Important	No	No	2
			CVE-2023-32044	Denial of Service	Important	No	No	2
			CVE-2023-35328	Elevation of Privilege	Important	No	No	2
			CVE-2023-32050	Elevation of Privilege	Important	No	No	2
5028228	高危	Microsoft Support for Windows	CVE-2023-35366	Remote Code Execution	Critical	No	No	2
			CVE-2023-33164	Denial of Service	Important	No	No	2

	Server 2012	CVE-2023-35365	Remote Code Execution	Critical	No	No	2
	R2, Windows	CVE-2023-32053	Elevation of Privilege	Important	No	No	2
	Embedded 8.1	CVE-2023-33169	Denial of Service	Important	No	No	2
	Industry Enterprise, Windows	CVE-2023-35340	Elevation of Privilege	Important	No	No	2
	Embedded 8.1	CVE-2023-35344	Remote Code Execution	Important	No	No	2
	Industry Pro	CVE-2023-35336	Security Feature Bypass	Important	No	No	2
		CVE-2023-35367	Remote Code Execution	Critical	No	No	2
		CVE-2023-35331	Denial of Service	Important	No	No	2
		CVE-2023-35330	Denial of Service	Important	No	No	2
		CVE-2023-32039	Information Disclosure	Important	No	No	2
		CVE-2023-33163	Remote Code Execution	Important	No	No	2
		CVE-2023-35342	Elevation of Privilege	Important	No	No	2
		CVE-2023-32085	Information Disclosure	Important	No	No	2
		CVE-2023-35346	Remote Code Execution	Important	No	No	2
		CVE-2023-33174	Information Disclosure	Important	No	No	2
		CVE-2023-35316	Information Disclosure	Important	No	No	2
		CVE-2023-35318	Denial of Service	Important	No	No	2
		CVE-2023-21756	Elevation of Privilege	Important	No	No	2
		CVE-2023-35352	Security Feature Bypass	Critical	No	No	1

		ADV230001	Defense in Depth	None	No	Yes	0
		CVE-2023-35322	Remote Code Execution	Important	No	No	2
		CVE-2023-35312	Elevation of Privilege	Important	No	No	1
		CVE-2023-32038	Remote Code Execution	Important	No	No	2
		CVE-2023-35309	Remote Code Execution	Important	No	No	2
		CVE-2023-35325	Information Disclosure	Important	No	No	2
		CVE-2023-32035	Denial of Service	Important	No	No	2
		CVE-2023-35317	Elevation of Privilege	Important	No	No	2
		CVE-2023-35302	Remote Code Execution	Important	No	No	2
		CVE-2023-35338	Denial of Service	Important	No	No	2
		CVE-2023-35306	Information Disclosure	Important	No	No	2
		CVE-2023-35308	Security Feature Bypass	Important	No	No	2
		CVE-2023-35351	Remote Code Execution	Important	No	No	2
		CVE-2023-35324	Information Disclosure	Important	No	No	2
		CVE-2023-35296	Information Disclosure	Important	No	No	2
		CVE-2023-35314	Denial of Service	Important	No	No	2
		CVE-2023-32033	Remote Code Execution	Important	No	No	2
		CVE-2023-32046	Elevation of Privilege	Important	No	Yes	0
		CVE-2023-35319	Denial of Service	Important	No	No	2
		CVE-2023-32040	Information Disclosure	Important	No	No	2

		CVE-2023-32057	Remote Code Execution	Critical	No	No	2
		CVE-2023-35360	Elevation of Privilege	Important	No	No	2
		CVE-2023-35300	Remote Code Execution	Important	No	No	2
		CVE-2023-35350	Remote Code Execution	Important	No	No	2
		CVE-2023-35303	Remote Code Execution	Important	No	No	2
		CVE-2023-32045	Denial of Service	Important	No	No	2
		CVE-2023-35341	Information Disclosure	Important	No	No	2
		CVE-2023-33154	Elevation of Privilege	Important	No	No	2
		CVE-2023-33173	Denial of Service	Important	No	No	2
		CVE-2023-33172	Denial of Service	Important	No	No	2
		CVE-2023-32034	Denial of Service	Important	No	No	2
		CVE-2023-35329	Denial of Service	Important	No	No	2
		ADV230002	Security Feature Bypass	Important	No	No	2
		CVE-2023-33168	Denial of Service	Important	No	No	2
		CVE-2023-21526	Information Disclosure	Important	No	No	1
		CVE-2023-36874	Elevation of Privilege	Important	No	Yes	0
		CVE-2023-35345	Remote Code Execution	Important	No	No	2
		CVE-2023-32055	Elevation of Privilege	Important	No	No	2
		CVE-2023-35310	Remote Code Execution	Important	No	No	2

			CVE-2023-35332	Security Feature Bypass	Important	No	No	2
			CVE-2023-35297	Remote Code Execution	Critical	No	No	2
			CVE-2023-35321	Denial of Service	Important	No	No	2
			CVE-2023-32043	Security Feature Bypass	Important	No	No	2
			CVE-2023-33167	Denial of Service	Important	No	No	2
			CVE-2023-33166	Denial of Service	Important	No	No	2
			CVE-2023-35299	Elevation of Privilege	Important	No	No	2
			CVE-2023-32044	Denial of Service	Important	No	No	2
			CVE-2023-35328	Elevation of Privilege	Important	No	No	2
			CVE-2023-32042	Information Disclosure	Important	No	No	2
			CVE-2023-35361	Elevation of Privilege	Important	No	No	2

本月微软发布的软件安全更新补丁共 16 个，详细列表如下：

KBID	奇安信集团等级	补丁名称	CVE 编号	漏洞的影响	漏洞等级	公开披露	已受攻击	漏洞的可利用性
5028167	高危	KB5028167: Cumulative security update for Internet Explorer	CVE-2023-35336	Security Feature Bypass	Important	No	No	2
			CVE-2023-35308	Security Feature Bypass	Important	No	No	2
			CVE-2023-32046	Elevation of Privilege	Important	No	Yes	0
5002069	高危	Description of the security update for Office 2013	CVE-2023-33152	Remote Code Execution	Important	No	No	2
5002406	高危	Description of the security update for Word 2016	CVE-2023-33150	Security Feature Bypass	Important	No	No	2
5002427	高危	Description of the security update for Outlook 2016	CVE-2023-35311	Security Feature Bypass	Important	No	Yes	0
			CVE-2023-33151	Spoofing	Important	No	No	2
4475581	高危	Description of the security update for Office 2016	CVE-2023-33153	Remote Code Execution	Important	No	No	2

5001952	高危	Description of the security update for Office 2013	CVE-2023-33149	Remote Code Execution	Important	No	No	2
4464506	高危	Description of the security update for Office 2013	CVE-2023-33153	Remote Code Execution	Important	No	No	2
5002419	高危	Description of the security update for Office 2016	CVE-2023-33149	Remote Code Execution	Important	No	No	2
5002058	高危	Description of the security update for Office 2016	CVE-2023-33152	Remote Code Execution	Important	No	No	2
5002426	高危	Description of the security update for Excel 2016	CVE-2023-33162	Information Disclosure	Important	No	No	2
5002434	高危	Description of the security update for Excel 2013	CVE-2023-33162	Information Disclosure	Important	No	No	2
5002425	高危	Description of the security update for SharePoint Enterprise	CVE-2023-33160	Remote Code Execution	Critical	No	No	2
			CVE-2023-33134	Remote Code Execution	Important	No	No	1
			CVE-2023-33159	Spoofing	Important	No	No	2

		Server 2016	CVE-2023-33157	Remote Code Execution	Critical	No	No	1
5002400	高危	Description of the security update for Office 2013	CVE-2023-33149	Remote Code Execution	Important	No	No	2
5002432	高危	Description of the security update for Outlook 2013	CVE-2023-35311	Security Feature Bypass	Important	No	Yes	0
			CVE-2023-33151	Spoofing	Important	No	No	2
4493154	高危	Description of the security update for Office 2016	CVE-2023-33149	Remote Code Execution	Important	No	No	2
5002411	高危	Description of the security update for Word 2013	CVE-2023-33150	Security Feature Bypass	Important	No	No	2

本月发布内容 4 个一般性更新补丁。

无

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>