

# 奇安信集团 2023 年 4 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 4 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.....	54

### 文档信息

文档名称	奇安信集团 2023 年 4 月补丁库更新通告		
文档编号	Qi An Xin Group-MSPatch-2023-0401		
发布日期	2023-04-12	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:2023.04.12.1,V10 版本:2023.04.12.1000)已发布,本次更新推送了 19 个微软安全补丁,修复了 77 个安全漏洞,其中 6 个微软官方评级为“严重(Critical)”,71 个评级为“重要(Important)”,这些漏洞影响 Windows、Office 等产品。

## 第2章 重点关注补丁

本月有 16 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
<a href="#">5025230</a>	CVE-2023-28220	Remote Code Execution	Critical	No	No	Exploitation More Likely
<a href="#">5025271</a>						
<a href="#">5025285</a>						
<a href="#">5025224</a>						
<a href="#">5025288</a>						
<a href="#">5025229</a>						
<a href="#">5025234</a>						
<a href="#">5025279</a>						
<a href="#">5025272</a>						
<a href="#">5025277</a>						
<a href="#">5025273</a>						
<a href="#">5025221</a>						
<a href="#">5025239</a>						
<a href="#">5025228</a>						
<a href="#">5025287</a>						
<a href="#">5025230</a>	CVE-2023-28252	Elevation of Privilege	Important	No	Yes	Exploitation Detected
<a href="#">5025271</a>						
<a href="#">5025285</a>						
<a href="#">5025224</a>						
<a href="#">5025288</a>						
<a href="#">5025229</a>						
<a href="#">5025234</a>						
<a href="#">5025279</a>						
<a href="#">5025272</a>						
<a href="#">5025277</a>						
<a href="#">5025273</a>						
<a href="#">5025221</a>						
<a href="#">5025239</a>						

<a href="#">5025228</a>						
<a href="#">5025287</a>						
<a href="#">5025230</a>	CVE-2023-28218	Elevation of Privilege	Important	No	No	Exploitation More Likely
<a href="#">5025271</a>						
<a href="#">5025285</a>						
<a href="#">5025224</a>						
<a href="#">5025288</a>						
<a href="#">5025229</a>						
<a href="#">5025234</a>						
<a href="#">5025279</a>						
<a href="#">5025272</a>						
<a href="#">5025277</a>						
<a href="#">5025273</a>						
<a href="#">5025221</a>						
<a href="#">5025239</a>						
<a href="#">5025228</a>						
<a href="#">5025287</a>						
<a href="#">5025230</a>	CVE-2023-28266	Information Disclosure	Important	No	No	Exploitation More Likely
<a href="#">5025271</a>						
<a href="#">5025285</a>						
<a href="#">5025224</a>						
<a href="#">5025288</a>						
<a href="#">5025229</a>						
<a href="#">5025234</a>						
<a href="#">5025279</a>						
<a href="#">5025272</a>						
<a href="#">5025277</a>						
<a href="#">5025273</a>						
<a href="#">5025221</a>						
<a href="#">5025239</a>						
<a href="#">5025228</a>						
<a href="#">5025287</a>						
<a href="#">5025230</a>	CVE-2023-28227	Remote Code Execution	Important	No	No	Exploitation More Likely
<a href="#">5025271</a>						
<a href="#">5025285</a>						
<a href="#">5025224</a>						
<a href="#">5025288</a>						
<a href="#">5025229</a>						
<a href="#">5025234</a>						
<a href="#">5025279</a>						
<a href="#">5025272</a>						

<a href="#">5025277</a>						
<a href="#">5025273</a>						
<a href="#">5025221</a>						
<a href="#">5025239</a>						
<a href="#">5025228</a>						
<a href="#">5025287</a>						
<a href="#">5025230</a>	CVE-2023-21554	Remote Code Execution	Critical	No	No	Exploitation More Likely
<a href="#">5025271</a>						
<a href="#">5025285</a>						
<a href="#">5025224</a>						
<a href="#">5025288</a>						
<a href="#">5025229</a>						
<a href="#">5025234</a>						
<a href="#">5025279</a>						
<a href="#">5025272</a>						
<a href="#">5025277</a>						
<a href="#">5025273</a>						
<a href="#">5025221</a>						
<a href="#">5025239</a>						
<a href="#">5025228</a>						
<a href="#">5025287</a>						
<a href="#">5025230</a>						
<a href="#">5025271</a>						
<a href="#">5025285</a>						
<a href="#">5025224</a>						
<a href="#">5025288</a>						
<a href="#">5025229</a>						
<a href="#">5025234</a>						
<a href="#">5025279</a>						
<a href="#">5025272</a>						
<a href="#">5025277</a>						
<a href="#">5025273</a>						
<a href="#">5025221</a>						
<a href="#">5025239</a>						
<a href="#">5025228</a>						
<a href="#">5025287</a>						
<a href="#">5025230</a>	CVE-2023-28219	Remote Code Execution	Critical	No	No	Exploitation More Likely
<a href="#">5025271</a>						
<a href="#">5025285</a>						
<a href="#">5025224</a>						
<a href="#">5025288</a>						

<a href="#">5025229</a>						
<a href="#">5025234</a>						
<a href="#">5025279</a>						
<a href="#">5025272</a>						
<a href="#">5025277</a>						
<a href="#">5025273</a>						
<a href="#">5025221</a>						
<a href="#">5025239</a>						
<a href="#">5025228</a>						
<a href="#">5025287</a>						
<a href="#">5025230</a>	CVE-2023-28274	Elevation of Privilege	Important	No	No	Exploitation More Likely
<a href="#">5025224</a>						
<a href="#">5025229</a>						
<a href="#">5025221</a>						
<a href="#">5025239</a>						
<a href="#">5025230</a>	CVE-2023-28232	Remote Code Execution	Critical	No	No	Exploitation Less Likely
<a href="#">5025271</a>						
<a href="#">5025285</a>						
<a href="#">5025224</a>						
<a href="#">5025288</a>						
<a href="#">5025229</a>						
<a href="#">5025234</a>						
<a href="#">5025279</a>						
<a href="#">5025272</a>						
<a href="#">5025277</a>						
<a href="#">5025273</a>						
<a href="#">5025221</a>						
<a href="#">5025239</a>						
<a href="#">5025228</a>						
<a href="#">5025287</a>						
<a href="#">5025230</a>	CVE-2023-28250	Remote Code Execution	Critical	No	No	Exploitation Less Likely
<a href="#">5025271</a>						
<a href="#">5025285</a>						
<a href="#">5025224</a>						
<a href="#">5025288</a>						
<a href="#">5025229</a>						
<a href="#">5025234</a>						
<a href="#">5025279</a>						
<a href="#">5025272</a>						
<a href="#">5025277</a>						
<a href="#">5025273</a>						



<a href="#">5025221</a>						
<a href="#">5025239</a>						
<a href="#">5025228</a>						
<a href="#">5025287</a>						
<a href="#">5025230</a>	CVE-2023-28231	Remote Code Execution	Critical	No	No	Exploitation More Likely
<a href="#">5025271</a>						
<a href="#">5025285</a>						
<a href="#">5025288</a>						
<a href="#">5025229</a>						
<a href="#">5025279</a>						
<a href="#">5025272</a>						
<a href="#">5025277</a>						
<a href="#">5025273</a>						
<a href="#">5025228</a>						
<a href="#">5025287</a>						

## 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
<a href="#">5025230</a>	高危	April 11, 2023—KB5025230 (OS Build 20348.1668) – Microsoft Support for Windows Server 2022	CVE-2023-21729	Information Disclosure	Important	No	No	2
			CVE-2023-28253	Information Disclosure	Important	No	No	2
			CVE-2023-28220	Remote Code Execution	Critical	No	No	1
			CVE-2023-28273	Elevation of Privilege	Important	No	No	2
			CVE-2023-28229	Elevation of Privilege	Important	No	No	2
			CVE-2023-28252	Elevation of Privilege	Important	No	Yes	0
			CVE-2023-24886	Remote Code Execution	Important	No	No	2
			CVE-2023-24927	Remote Code Execution	Important	No	No	2
			CVE-2023-24924	Remote Code Execution	Important	No	No	2
			CVE-2023-28218	Elevation of Privilege	Important	No	No	1
			CVE-2023-28293	Elevation of Privilege	Important	No	No	2
			CVE-2023-28277	Information Disclosure	Important	No	No	2
			CVE-2023-28308	Remote Code Execution	Important	No	No	2
			CVE-2023-28266	Information Disclosure	Important	No	No	1
			CVE-2023-28240	Remote Code Execution	Important	No	No	2

			CVE-2023-28236	Elevation of Privilege	Important	No	No	2
			CVE-2023-28227	Remote Code Execution	Important	No	No	1
			CVE-2023-28217	Denial of Service	Important	No	No	2
			CVE-2023-24931	Denial of Service	Important	No	No	2
			CVE-2023-28233	Denial of Service	Important	No	No	2
			CVE-2023-28298	Denial of Service	Important	No	No	2
			CVE-2023-21554	Remote Code Execution	Critical	No	No	1
			CVE-2023-28256	Remote Code Execution	Important	No	No	2
			CVE-2023-28216	Elevation of Privilege	Important	No	No	2
			CVE-2023-28249	Security Feature Bypass	Important	No	No	2
			CVE-2023-28302	Denial of Service	Important	No	No	2
			CVE-2023-28271	Information Disclosure	Important	No	No	2
			CVE-2023-28228	Spoofing	Important	No	No	2
			CVE-2023-28275	Remote Code Execution	Important	No	No	2
			CVE-2023-28255	Remote Code Execution	Important	No	No	2
			CVE-2023-28223	Remote Code Execution	Important	No	No	2
			CVE-2023-28234	Denial of Service	Important	No	No	2
			CVE-2023-24885	Remote Code Execution	Important	No	No	2
			CVE-2023-28225	Elevation of Privilege	Important	No	No	2
			CVE-2023-28248	Elevation of Privilege	Important	No	No	2

			CVE-2023-28270	Security Feature Bypass	Important	No	No	2
			CVE-2023-28305	Remote Code Execution	Important	No	No	2
			CVE-2023-24883	Information Disclosure	Important	No	No	2
			CVE-2023-24912	Elevation of Privilege	Important	No	No	1
			CVE-2023-21727	Remote Code Execution	Important	No	No	2
			CVE-2023-28219	Remote Code Execution	Critical	No	No	1
			CVE-2023-28274	Elevation of Privilege	Important	No	No	1
			CVE-2023-28224	Remote Code Execution	Important	No	No	2
			CVE-2023-28232	Remote Code Execution	Critical	No	No	2
			CVE-2023-28254	Remote Code Execution	Important	No	No	2
			CVE-2023-24884	Remote Code Execution	Important	No	No	2
			CVE-2023-28268	Elevation of Privilege	Important	No	No	2
			CVE-2023-28238	Remote Code Execution	Important	No	No	2
			CVE-2023-28222	Elevation of Privilege	Important	No	No	2
			CVE-2023-24929	Remote Code Execution	Important	No	No	2
			CVE-2023-28267	Information Disclosure	Important	No	No	2
			CVE-2023-24926	Remote Code Execution	Important	No	No	2
			CVE-2023-28244	Elevation of Privilege	Important	No	No	2
			CVE-2023-28237	Remote Code Execution	Important	No	No	2
			CVE-2023-21769	Denial of Service	Important	No	No	2

			CVE-2023-28250	Remote Code Execution	Critical	No	No	2
			CVE-2023-24925	Remote Code Execution	Important	No	No	2
			CVE-2023-24928	Remote Code Execution	Important	No	No	2
			CVE-2023-28247	Information Disclosure	Important	No	No	2
			CVE-2023-28241	Denial of Service	Important	No	No	2
			CVE-2023-28276	Security Feature Bypass	Important	No	No	2
			CVE-2023-28272	Elevation of Privilege	Important	No	No	2
			CVE-2023-28306	Remote Code Execution	Important	No	No	2
			CVE-2023-28246	Elevation of Privilege	Important	No	No	2
			CVE-2023-28269	Security Feature Bypass	Important	No	No	2
			CVE-2023-28231	Remote Code Execution	Critical	No	No	1
			CVE-2023-28278	Remote Code Execution	Important	No	No	2
			CVE-2023-28307	Remote Code Execution	Important	No	No	2
			CVE-2023-24887	Remote Code Execution	Important	No	No	2
			CVE-2023-28243	Remote Code Execution	Important	No	No	2
			CVE-2023-28221	Elevation of Privilege	Important	No	No	2
<a href="#">5025271</a>	高危	April 11, 2023—KB5025271 (Monthly	CVE-2023-21729	Information Disclosure	Important	No	No	2
			CVE-2023-28253	Information Disclosure	Important	No	No	2
			CVE-2023-28220	Remote Code Execution	Critical	No	No	1

		Rollup)	CVE-2023-28229	Elevation of Privilege	Important	No	No	2
		-						
		Microsoft	CVE-2023-28252	Elevation of Privilege	Important	No	Yes	0
		Support for	CVE-2023-28218	Elevation of Privilege	Important	No	No	1
		Windows Server	CVE-2023-28293	Elevation of Privilege	Important	No	No	2
		2008	CVE-2023-28266	Information Disclosure	Important	No	No	1
		Datacenter	CVE-2023-28308	Remote Code Execution	Important	No	No	2
		ESU, Windows	CVE-2023-28240	Remote Code Execution	Important	No	No	2
		Server	CVE-2023-28217	Denial of Service	Important	No	No	2
		2008	CVE-2023-28227	Remote Code Execution	Important	No	No	1
		Standard	CVE-2023-28298	Denial of Service	Important	No	No	2
		ESU, Windows	CVE-2023-21554	Remote Code Execution	Critical	No	No	1
		Server	CVE-2023-28256	Remote Code Execution	Important	No	No	2
		2008	CVE-2023-28216	Elevation of Privilege	Important	No	No	2
		Enterprise	CVE-2023-28302	Denial of Service	Important	No	No	2
		ESU	CVE-2023-28271	Information Disclosure	Important	No	No	2
			CVE-2023-28228	Spoofing	Important	No	No	2
			CVE-2023-28275	Remote Code Execution	Important	No	No	2
			CVE-2023-28255	Remote Code Execution	Important	No	No	2
			CVE-2023-28223	Remote Code Execution	Important	No	No	2
			CVE-2023-28305	Remote Code Execution	Important	No	No	2
			CVE-2023-24912	Elevation of Privilege	Important	No	No	1

			CVE-2023-21727	Remote Code Execution	Important	No	No	2
			CVE-2023-28219	Remote Code Execution	Critical	No	No	1
			CVE-2023-28232	Remote Code Execution	Critical	No	No	2
			CVE-2023-28254	Remote Code Execution	Important	No	No	2
			CVE-2023-28268	Elevation of Privilege	Important	No	No	2
			CVE-2023-28222	Elevation of Privilege	Important	No	No	2
			CVE-2023-28244	Elevation of Privilege	Important	No	No	2
			CVE-2023-21769	Denial of Service	Important	No	No	2
			CVE-2023-28250	Remote Code Execution	Critical	No	No	2
			CVE-2023-28241	Denial of Service	Important	No	No	2
			CVE-2023-28276	Security Feature Bypass	Important	No	No	2
			CVE-2023-28272	Elevation of Privilege	Important	No	No	2
			CVE-2023-28306	Remote Code Execution	Important	No	No	2
			CVE-2023-28231	Remote Code Execution	Critical	No	No	1
			CVE-2023-28278	Remote Code Execution	Important	No	No	2
			CVE-2023-28307	Remote Code Execution	Important	No	No	2
<a href="#">5025285</a>	高危	April 11, 2023—KB5025285 (Monthly Rollup) -	CVE-2023-21729	Information Disclosure	Important	No	No	2
			CVE-2023-28253	Information Disclosure	Important	No	No	2
			CVE-2023-28220	Remote Code Execution	Critical	No	No	1
			CVE-2023-28229	Elevation of Privilege	Important	No	No	2



Microsoft Support for Windows Server 2012 R2	CVE-2023-28252	Elevation of Privilege	Important	No	Yes	0
	CVE-2023-24886	Remote Code Execution	Important	No	No	2
	CVE-2023-24927	Remote Code Execution	Important	No	No	2
	CVE-2023-24924	Remote Code Execution	Important	No	No	2
	CVE-2023-28218	Elevation of Privilege	Important	No	No	1
	CVE-2023-28293	Elevation of Privilege	Important	No	No	2
	CVE-2023-28266	Information Disclosure	Important	No	No	1
	CVE-2023-28308	Remote Code Execution	Important	No	No	2
	CVE-2023-28240	Remote Code Execution	Important	No	No	2
	CVE-2023-28236	Elevation of Privilege	Important	No	No	2
	CVE-2023-28217	Denial of Service	Important	No	No	2
	CVE-2023-28227	Remote Code Execution	Important	No	No	1
	CVE-2023-24931	Denial of Service	Important	No	No	2
	CVE-2023-28298	Denial of Service	Important	No	No	2
	CVE-2023-21554	Remote Code Execution	Critical	No	No	1
	CVE-2023-28256	Remote Code Execution	Important	No	No	2
	CVE-2023-28216	Elevation of Privilege	Important	No	No	2
	CVE-2023-28249	Security Feature Bypass	Important	No	No	2
	CVE-2023-28302	Denial of Service	Important	No	No	2
	CVE-2023-28271	Information Disclosure	Important	No	No	2

			CVE-2023-28228	Spoofing	Important	No	No	2
			CVE-2023-28275	Remote Code Execution	Important	No	No	2
			CVE-2023-28255	Remote Code Execution	Important	No	No	2
			CVE-2023-28223	Remote Code Execution	Important	No	No	2
			CVE-2023-24885	Remote Code Execution	Important	No	No	2
			CVE-2023-28305	Remote Code Execution	Important	No	No	2
			CVE-2023-24883	Information Disclosure	Important	No	No	2
			CVE-2023-24912	Elevation of Privilege	Important	No	No	1
			CVE-2023-21727	Remote Code Execution	Important	No	No	2
			CVE-2023-28219	Remote Code Execution	Critical	No	No	1
			CVE-2023-28224	Remote Code Execution	Important	No	No	2
			CVE-2023-28232	Remote Code Execution	Critical	No	No	2
			CVE-2023-28254	Remote Code Execution	Important	No	No	2
			CVE-2023-24884	Remote Code Execution	Important	No	No	2
			CVE-2023-28268	Elevation of Privilege	Important	No	No	2
			CVE-2023-28238	Remote Code Execution	Important	No	No	2
			CVE-2023-28222	Elevation of Privilege	Important	No	No	2
			CVE-2023-24929	Remote Code Execution	Important	No	No	2
			CVE-2023-28267	Information Disclosure	Important	No	No	2
			CVE-2023-24926	Remote Code Execution	Important	No	No	2
			CVE-2023-28244	Elevation of Privilege	Important	No	No	2

			CVE-2023-28237	Remote Code Execution	Important	No	No	2
			CVE-2023-21769	Denial of Service	Important	No	No	2
			CVE-2023-28250	Remote Code Execution	Critical	No	No	2
			CVE-2023-24925	Remote Code Execution	Important	No	No	2
			CVE-2023-24928	Remote Code Execution	Important	No	No	2
			CVE-2023-28247	Information Disclosure	Important	No	No	2
			CVE-2023-28241	Denial of Service	Important	No	No	2
			CVE-2023-28276	Security Feature Bypass	Important	No	No	2
			CVE-2023-28272	Elevation of Privilege	Important	No	No	2
			CVE-2023-28306	Remote Code Execution	Important	No	No	2
			CVE-2023-28269	Security Feature Bypass	Important	No	No	2
			CVE-2023-28231	Remote Code Execution	Critical	No	No	1
			CVE-2023-24887	Remote Code Execution	Important	No	No	2
			CVE-2023-28278	Remote Code Execution	Important	No	No	2
			CVE-2023-28307	Remote Code Execution	Important	No	No	2
			CVE-2023-28243	Remote Code Execution	Important	No	No	2
<a href="#">5025224</a>	高危	April 11, 2023—KB5025224 (OS Build	CVE-2023-21729	Information Disclosure	Important	No	No	2
			CVE-2023-28253	Information Disclosure	Important	No	No	2
			CVE-2023-28220	Remote Code Execution	Critical	No	No	1

	22000.18 17) - Microsoft Support for Windows 11 version 21H2, all editions	CVE-2023-28273	Elevation of Privilege	Important	No	No	2
		CVE-2023-28229	Elevation of Privilege	Important	No	No	2
		CVE-2023-28252	Elevation of Privilege	Important	No	Yes	0
		CVE-2023-24886	Remote Code Execution	Important	No	No	2
		CVE-2023-24927	Remote Code Execution	Important	No	No	2
		CVE-2023-24924	Remote Code Execution	Important	No	No	2
		CVE-2023-28218	Elevation of Privilege	Important	No	No	1
		CVE-2023-28293	Elevation of Privilege	Important	No	No	2
		CVE-2023-28266	Information Disclosure	Important	No	No	1
		CVE-2023-28236	Elevation of Privilege	Important	No	No	2
		CVE-2023-28217	Denial of Service	Important	No	No	2
		CVE-2023-28227	Remote Code Execution	Important	No	No	1
		CVE-2023-24931	Denial of Service	Important	No	No	2
		CVE-2023-28233	Denial of Service	Important	No	No	2
		CVE-2023-28298	Denial of Service	Important	No	No	2
		CVE-2023-21554	Remote Code Execution	Critical	No	No	1
		CVE-2023-28216	Elevation of Privilege	Important	No	No	2
		CVE-2023-28249	Security Feature Bypass	Important	No	No	2
		CVE-2023-28302	Denial of Service	Important	No	No	2
		CVE-2023-28271	Information Disclosure	Important	No	No	2

			CVE-2023-28228	Spoofing	Important	No	No	2
			CVE-2023-28275	Remote Code Execution	Important	No	No	2
			CVE-2023-24885	Remote Code Execution	Important	No	No	2
			CVE-2023-28234	Denial of Service	Important	No	No	2
			CVE-2023-28225	Elevation of Privilege	Important	No	No	2
			CVE-2023-28248	Elevation of Privilege	Important	No	No	2
			CVE-2023-28226	Security Feature Bypass	Important	No	No	2
			CVE-2023-28270	Security Feature Bypass	Important	No	No	2
			CVE-2023-24883	Information Disclosure	Important	No	No	2
			CVE-2023-24912	Elevation of Privilege	Important	No	No	1
			CVE-2023-21727	Remote Code Execution	Important	No	No	2
			CVE-2023-28219	Remote Code Execution	Critical	No	No	1
			CVE-2023-28274	Elevation of Privilege	Important	No	No	1
			CVE-2023-28224	Remote Code Execution	Important	No	No	2
			CVE-2023-28232	Remote Code Execution	Critical	No	No	2
			CVE-2023-24884	Remote Code Execution	Important	No	No	2
			CVE-2023-28238	Remote Code Execution	Important	No	No	2
			CVE-2023-28222	Elevation of Privilege	Important	No	No	2
			CVE-2023-24929	Remote Code Execution	Important	No	No	2
			CVE-2023-28267	Information Disclosure	Important	No	No	2

			CVE-2023-24926	Remote Code Execution	Important	No	No	2
			CVE-2023-28237	Remote Code Execution	Important	No	No	2
			CVE-2023-21769	Denial of Service	Important	No	No	2
			CVE-2023-28250	Remote Code Execution	Critical	No	No	2
			CVE-2023-24925	Remote Code Execution	Important	No	No	2
			CVE-2023-24928	Remote Code Execution	Important	No	No	2
			CVE-2023-28241	Denial of Service	Important	No	No	2
			CVE-2023-28276	Security Feature Bypass	Important	No	No	2
			CVE-2023-28272	Elevation of Privilege	Important	No	No	2
			CVE-2023-28246	Elevation of Privilege	Important	No	No	2
			CVE-2023-28269	Security Feature Bypass	Important	No	No	2
			CVE-2023-24887	Remote Code Execution	Important	No	No	2
			CVE-2023-28243	Remote Code Execution	Important	No	No	2
			CVE-2023-28221	Elevation of Privilege	Important	No	No	2
<a href="#">5025288</a>	高危	April 11, 2023—KB5025288 (Security-only update) - Microsoft	CVE-2023-21729	Information Disclosure	Important	No	No	2
			CVE-2023-28253	Information Disclosure	Important	No	No	2
			CVE-2023-28220	Remote Code Execution	Critical	No	No	1
			CVE-2023-28229	Elevation of Privilege	Important	No	No	2
			CVE-2023-28252	Elevation of Privilege	Important	No	Yes	0

t Support for Windows Server 2012 R2	CVE-2023-24886	Remote Code Execution	Important	No	No	2
	CVE-2023-24927	Remote Code Execution	Important	No	No	2
	CVE-2023-24924	Remote Code Execution	Important	No	No	2
	CVE-2023-28218	Elevation of Privilege	Important	No	No	1
	CVE-2023-28293	Elevation of Privilege	Important	No	No	2
	CVE-2023-28266	Information Disclosure	Important	No	No	1
	CVE-2023-28308	Remote Code Execution	Important	No	No	2
	CVE-2023-28240	Remote Code Execution	Important	No	No	2
	CVE-2023-28236	Elevation of Privilege	Important	No	No	2
	CVE-2023-28217	Denial of Service	Important	No	No	2
	CVE-2023-28227	Remote Code Execution	Important	No	No	1
	CVE-2023-24931	Denial of Service	Important	No	No	2
	CVE-2023-28298	Denial of Service	Important	No	No	2
	CVE-2023-21554	Remote Code Execution	Critical	No	No	1
	CVE-2023-28256	Remote Code Execution	Important	No	No	2
	CVE-2023-28216	Elevation of Privilege	Important	No	No	2
	CVE-2023-28249	Security Feature Bypass	Important	No	No	2
	CVE-2023-28302	Denial of Service	Important	No	No	2
	CVE-2023-28271	Information Disclosure	Important	No	No	2
	CVE-2023-28228	Spoofing	Important	No	No	2

			CVE-2023-28275	Remote Code Execution	Important	No	No	2
			CVE-2023-28255	Remote Code Execution	Important	No	No	2
			CVE-2023-28223	Remote Code Execution	Important	No	No	2
			CVE-2023-24885	Remote Code Execution	Important	No	No	2
			CVE-2023-28305	Remote Code Execution	Important	No	No	2
			CVE-2023-24883	Information Disclosure	Important	No	No	2
			CVE-2023-24912	Elevation of Privilege	Important	No	No	1
			CVE-2023-21727	Remote Code Execution	Important	No	No	2
			CVE-2023-28219	Remote Code Execution	Critical	No	No	1
			CVE-2023-28224	Remote Code Execution	Important	No	No	2
			CVE-2023-28232	Remote Code Execution	Critical	No	No	2
			CVE-2023-28254	Remote Code Execution	Important	No	No	2
			CVE-2023-24884	Remote Code Execution	Important	No	No	2
			CVE-2023-28268	Elevation of Privilege	Important	No	No	2
			CVE-2023-28238	Remote Code Execution	Important	No	No	2
			CVE-2023-28222	Elevation of Privilege	Important	No	No	2
			CVE-2023-24929	Remote Code Execution	Important	No	No	2
			CVE-2023-28267	Information Disclosure	Important	No	No	2
			CVE-2023-24926	Remote Code Execution	Important	No	No	2
			CVE-2023-28244	Elevation of Privilege	Important	No	No	2



			CVE-2023-28237	Remote Code Execution	Important	No	No	2
			CVE-2023-21769	Denial of Service	Important	No	No	2
			CVE-2023-28250	Remote Code Execution	Critical	No	No	2
			CVE-2023-24925	Remote Code Execution	Important	No	No	2
			CVE-2023-24928	Remote Code Execution	Important	No	No	2
			CVE-2023-28247	Information Disclosure	Important	No	No	2
			CVE-2023-28241	Denial of Service	Important	No	No	2
			CVE-2023-28276	Security Feature Bypass	Important	No	No	2
			CVE-2023-28272	Elevation of Privilege	Important	No	No	2
			CVE-2023-28306	Remote Code Execution	Important	No	No	2
			CVE-2023-28269	Security Feature Bypass	Important	No	No	2
			CVE-2023-28231	Remote Code Execution	Critical	No	No	1
			CVE-2023-24887	Remote Code Execution	Important	No	No	2
			CVE-2023-28278	Remote Code Execution	Important	No	No	2
			CVE-2023-28307	Remote Code Execution	Important	No	No	2
			CVE-2023-28243	Remote Code Execution	Important	No	No	2
<a href="#">5025229</a>	高危	April 11, 2023—KB5025229 (OS Build	CVE-2023-21729	Information Disclosure	Important	No	No	2
			CVE-2023-28253	Information Disclosure	Important	No	No	2
			CVE-2023-28220	Remote Code Execution	Critical	No	No	1

	17763.4252) - Microsoft Support for Windows Server 2019	CVE-2023-28273	Elevation of Privilege	Important	No	No	2
		CVE-2023-28229	Elevation of Privilege	Important	No	No	2
		CVE-2023-28252	Elevation of Privilege	Important	No	Yes	0
		CVE-2023-24886	Remote Code Execution	Important	No	No	2
		CVE-2023-24927	Remote Code Execution	Important	No	No	2
		CVE-2023-24924	Remote Code Execution	Important	No	No	2
		CVE-2023-28218	Elevation of Privilege	Important	No	No	1
		CVE-2023-28293	Elevation of Privilege	Important	No	No	2
		CVE-2023-28266	Information Disclosure	Important	No	No	1
		CVE-2023-28308	Remote Code Execution	Important	No	No	2
		CVE-2023-28240	Remote Code Execution	Important	No	No	2
		CVE-2023-28236	Elevation of Privilege	Important	No	No	2
		CVE-2023-28217	Denial of Service	Important	No	No	2
		CVE-2023-28227	Remote Code Execution	Important	No	No	1
		CVE-2023-28235	Security Feature Bypass	Important	No	No	2
		CVE-2023-24931	Denial of Service	Important	No	No	2
		CVE-2023-28298	Denial of Service	Important	No	No	2
		CVE-2023-21554	Remote Code Execution	Critical	No	No	1
		CVE-2023-28256	Remote Code Execution	Important	No	No	2
		CVE-2023-28216	Elevation of Privilege	Important	No	No	2

			CVE-2023-28249	Security Feature Bypass	Important	No	No	2
			CVE-2023-28302	Denial of Service	Important	No	No	2
			CVE-2023-28271	Information Disclosure	Important	No	No	2
			CVE-2023-28228	Spoofing	Important	No	No	2
			CVE-2023-28275	Remote Code Execution	Important	No	No	2
			CVE-2023-28255	Remote Code Execution	Important	No	No	2
			CVE-2023-28223	Remote Code Execution	Important	No	No	2
			CVE-2023-24885	Remote Code Execution	Important	No	No	2
			CVE-2023-28225	Elevation of Privilege	Important	No	No	2
			CVE-2023-28248	Elevation of Privilege	Important	No	No	2
			CVE-2023-28226	Security Feature Bypass	Important	No	No	2
			CVE-2023-28270	Security Feature Bypass	Important	No	No	2
			CVE-2023-28305	Remote Code Execution	Important	No	No	2
			CVE-2023-24883	Information Disclosure	Important	No	No	2
			CVE-2023-24912	Elevation of Privilege	Important	No	No	1
			CVE-2023-21727	Remote Code Execution	Important	No	No	2
			CVE-2023-28219	Remote Code Execution	Critical	No	No	1
			CVE-2023-28274	Elevation of Privilege	Important	No	No	1
			CVE-2023-28224	Remote Code Execution	Important	No	No	2

			CVE-2023-28232	Remote Code Execution	Critical	No	No	2
			CVE-2023-28254	Remote Code Execution	Important	No	No	2
			CVE-2023-24884	Remote Code Execution	Important	No	No	2
			CVE-2023-28268	Elevation of Privilege	Important	No	No	2
			CVE-2023-28238	Remote Code Execution	Important	No	No	2
			CVE-2023-28222	Elevation of Privilege	Important	No	No	2
			CVE-2023-24929	Remote Code Execution	Important	No	No	2
			CVE-2023-28267	Information Disclosure	Important	No	No	2
			CVE-2023-24926	Remote Code Execution	Important	No	No	2
			CVE-2023-28244	Elevation of Privilege	Important	No	No	2
			CVE-2023-28237	Remote Code Execution	Important	No	No	2
			CVE-2023-21769	Denial of Service	Important	No	No	2
			CVE-2023-28250	Remote Code Execution	Critical	No	No	2
			CVE-2023-24925	Remote Code Execution	Important	No	No	2
			CVE-2023-24928	Remote Code Execution	Important	No	No	2
			CVE-2023-28247	Information Disclosure	Important	No	No	2
			CVE-2023-28241	Denial of Service	Important	No	No	2
			CVE-2023-28276	Security Feature Bypass	Important	No	No	2
			CVE-2023-28272	Elevation of Privilege	Important	No	No	2
			CVE-2023-28306	Remote Code Execution	Important	No	No	2

			CVE-2023-28269	Security Feature Bypass	Important	No	No	2
			CVE-2023-28231	Remote Code Execution	Critical	No	No	1
			CVE-2023-24887	Remote Code Execution	Important	No	No	2
			CVE-2023-28278	Remote Code Execution	Important	No	No	2
			CVE-2023-28307	Remote Code Execution	Important	No	No	2
			CVE-2023-28243	Remote Code Execution	Important	No	No	2
			CVE-2023-28221	Elevation of Privilege	Important	No	No	2
<a href="#">5025234</a>	高危	April 11, 2023—KB5025234 (OS Build 10240.19869) – Microsoft Support for Windows 10	CVE-2023-21729	Information Disclosure	Important	No	No	2
			CVE-2023-28253	Information Disclosure	Important	No	No	2
			CVE-2023-28220	Remote Code Execution	Critical	No	No	1
			CVE-2023-28229	Elevation of Privilege	Important	No	No	2
			CVE-2023-28252	Elevation of Privilege	Important	No	Yes	0
			CVE-2023-24886	Remote Code Execution	Important	No	No	2
			CVE-2023-24927	Remote Code Execution	Important	No	No	2
			CVE-2023-24924	Remote Code Execution	Important	No	No	2
			CVE-2023-28218	Elevation of Privilege	Important	No	No	1
			CVE-2023-28293	Elevation of Privilege	Important	No	No	2
			CVE-2023-28266	Information Disclosure	Important	No	No	1
			CVE-2023-28236	Elevation of Privilege	Important	No	No	2
			CVE-2023-28217	Denial of Service	Important	No	No	2

			CVE-2023-28227	Remote Code Execution	Important	No	No	1
			CVE-2023-24931	Denial of Service	Important	No	No	2
			CVE-2023-28298	Denial of Service	Important	No	No	2
			CVE-2023-21554	Remote Code Execution	Critical	No	No	1
			CVE-2023-28216	Elevation of Privilege	Important	No	No	2
			CVE-2023-28249	Security Feature Bypass	Important	No	No	2
			CVE-2023-28302	Denial of Service	Important	No	No	2
			CVE-2023-28271	Information Disclosure	Important	No	No	2
			CVE-2023-28228	Spoofing	Important	No	No	2
			CVE-2023-28275	Remote Code Execution	Important	No	No	2
			CVE-2023-24885	Remote Code Execution	Important	No	No	2
			CVE-2023-28225	Elevation of Privilege	Important	No	No	2
			CVE-2023-28226	Security Feature Bypass	Important	No	No	2
			CVE-2023-24883	Information Disclosure	Important	No	No	2
			CVE-2023-24912	Elevation of Privilege	Important	No	No	1
			CVE-2023-21727	Remote Code Execution	Important	No	No	2
			CVE-2023-28219	Remote Code Execution	Critical	No	No	1
			CVE-2023-28224	Remote Code Execution	Important	No	No	2
			CVE-2023-28232	Remote Code Execution	Critical	No	No	2
			CVE-2023-24884	Remote Code Execution	Important	No	No	2

			CVE-2023-28238	Remote Code Execution	Important	No	No	2
			CVE-2023-28222	Elevation of Privilege	Important	No	No	2
			CVE-2023-24929	Remote Code Execution	Important	No	No	2
			CVE-2023-28267	Information Disclosure	Important	No	No	2
			CVE-2023-24926	Remote Code Execution	Important	No	No	2
			CVE-2023-28237	Remote Code Execution	Important	No	No	2
			CVE-2023-21769	Denial of Service	Important	No	No	2
			CVE-2023-28250	Remote Code Execution	Critical	No	No	2
			CVE-2023-24925	Remote Code Execution	Important	No	No	2
			CVE-2023-24928	Remote Code Execution	Important	No	No	2
			CVE-2023-28241	Denial of Service	Important	No	No	2
			CVE-2023-28276	Security Feature Bypass	Important	No	No	2
			CVE-2023-28272	Elevation of Privilege	Important	No	No	2
			CVE-2023-28269	Security Feature Bypass	Important	No	No	2
			CVE-2023-24887	Remote Code Execution	Important	No	No	2
			CVE-2023-28243	Remote Code Execution	Important	No	No	2
			CVE-2023-28221	Elevation of Privilege	Important	No	No	2
<a href="#">5025279</a>	高危	April 11, 2023—KB502527	CVE-2023-21729	Information Disclosure	Important	No	No	2
			CVE-2023-28253	Information Disclosure	Important	No	No	2

	9 (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-2023-28220	Remote Code Execution	Critical	No	No	1
		CVE-2023-28229	Elevation of Privilege	Important	No	No	2
		CVE-2023-28252	Elevation of Privilege	Important	No	Yes	0
		CVE-2023-28218	Elevation of Privilege	Important	No	No	1
		CVE-2023-28293	Elevation of Privilege	Important	No	No	2
		CVE-2023-28266	Information Disclosure	Important	No	No	1
		CVE-2023-28308	Remote Code Execution	Important	No	No	2
		CVE-2023-28240	Remote Code Execution	Important	No	No	2
		CVE-2023-28217	Denial of Service	Important	No	No	2
		CVE-2023-28227	Remote Code Execution	Important	No	No	1
		CVE-2023-24931	Denial of Service	Important	No	No	2
		CVE-2023-28298	Denial of Service	Important	No	No	2
		CVE-2023-21554	Remote Code Execution	Critical	No	No	1
		CVE-2023-28256	Remote Code Execution	Important	No	No	2
		CVE-2023-28216	Elevation of Privilege	Important	No	No	2
		CVE-2023-28302	Denial of Service	Important	No	No	2
		CVE-2023-28271	Information Disclosure	Important	No	No	2
		CVE-2023-28228	Spoofing	Important	No	No	2
		CVE-2023-28275	Remote Code Execution	Important	No	No	2
		CVE-2023-28255	Remote Code Execution	Important	No	No	2
CVE-2023-28223	Remote Code Execution	Important	No	No	2		



			CVE-2023-28305	Remote Code Execution	Important	No	No	2
			CVE-2023-24912	Elevation of Privilege	Important	No	No	1
			CVE-2023-21727	Remote Code Execution	Important	No	No	2
			CVE-2023-28219	Remote Code Execution	Critical	No	No	1
			CVE-2023-28232	Remote Code Execution	Critical	No	No	2
			CVE-2023-28254	Remote Code Execution	Important	No	No	2
			CVE-2023-28268	Elevation of Privilege	Important	No	No	2
			CVE-2023-28238	Remote Code Execution	Important	No	No	2
			CVE-2023-28222	Elevation of Privilege	Important	No	No	2
			CVE-2023-28267	Information Disclosure	Important	No	No	2
			CVE-2023-28244	Elevation of Privilege	Important	No	No	2
			CVE-2023-21769	Denial of Service	Important	No	No	2
			CVE-2023-28250	Remote Code Execution	Critical	No	No	2
			CVE-2023-28241	Denial of Service	Important	No	No	2
			CVE-2023-28276	Security Feature Bypass	Important	No	No	2
			CVE-2023-28272	Elevation of Privilege	Important	No	No	2
			CVE-2023-28306	Remote Code Execution	Important	No	No	2
			CVE-2023-28231	Remote Code Execution	Critical	No	No	1
			CVE-2023-28278	Remote Code Execution	Important	No	No	2
			CVE-2023-28307	Remote Code Execution	Important	No	No	2

<a href="#">5025272</a>	高危	April 11, 2023—KB502527 2 (Security-only update) – Microsoft Support for Windows Server 2012	CVE-2023-21729	Information Disclosure	Important	No	No	2
			CVE-2023-28253	Information Disclosure	Important	No	No	2
			CVE-2023-28220	Remote Code Execution	Critical	No	No	1
			CVE-2023-28229	Elevation of Privilege	Important	No	No	2
			CVE-2023-28252	Elevation of Privilege	Important	No	Yes	0
			CVE-2023-24886	Remote Code Execution	Important	No	No	2
			CVE-2023-24927	Remote Code Execution	Important	No	No	2
			CVE-2023-24924	Remote Code Execution	Important	No	No	2
			CVE-2023-28218	Elevation of Privilege	Important	No	No	1
			CVE-2023-28293	Elevation of Privilege	Important	No	No	2
			CVE-2023-28266	Information Disclosure	Important	No	No	1
			CVE-2023-28308	Remote Code Execution	Important	No	No	2
			CVE-2023-28240	Remote Code Execution	Important	No	No	2
			CVE-2023-28236	Elevation of Privilege	Important	No	No	2
			CVE-2023-28217	Denial of Service	Important	No	No	2
			CVE-2023-28227	Remote Code Execution	Important	No	No	1
			CVE-2023-24931	Denial of Service	Important	No	No	2
			CVE-2023-28298	Denial of Service	Important	No	No	2
			CVE-2023-21554	Remote Code Execution	Critical	No	No	1
			CVE-2023-28256	Remote Code Execution	Important	No	No	2

			CVE-2023-28216	Elevation of Privilege	Important	No	No	2
			CVE-2023-28249	Security Feature Bypass	Important	No	No	2
			CVE-2023-28302	Denial of Service	Important	No	No	2
			CVE-2023-28271	Information Disclosure	Important	No	No	2
			CVE-2023-28228	Spoofing	Important	No	No	2
			CVE-2023-28275	Remote Code Execution	Important	No	No	2
			CVE-2023-28255	Remote Code Execution	Important	No	No	2
			CVE-2023-28223	Remote Code Execution	Important	No	No	2
			CVE-2023-24885	Remote Code Execution	Important	No	No	2
			CVE-2023-28305	Remote Code Execution	Important	No	No	2
			CVE-2023-24883	Information Disclosure	Important	No	No	2
			CVE-2023-24912	Elevation of Privilege	Important	No	No	1
			CVE-2023-21727	Remote Code Execution	Important	No	No	2
			CVE-2023-28219	Remote Code Execution	Critical	No	No	1
			CVE-2023-28224	Remote Code Execution	Important	No	No	2
			CVE-2023-28232	Remote Code Execution	Critical	No	No	2
			CVE-2023-28254	Remote Code Execution	Important	No	No	2
			CVE-2023-24884	Remote Code Execution	Important	No	No	2
			CVE-2023-28268	Elevation of Privilege	Important	No	No	2
			CVE-2023-28238	Remote Code Execution	Important	No	No	2

			CVE-2023-28222	Elevation of Privilege	Important	No	No	2
			CVE-2023-24929	Remote Code Execution	Important	No	No	2
			CVE-2023-28267	Information Disclosure	Important	No	No	2
			CVE-2023-24926	Remote Code Execution	Important	No	No	2
			CVE-2023-28244	Elevation of Privilege	Important	No	No	2
			CVE-2023-28237	Remote Code Execution	Important	No	No	2
			CVE-2023-21769	Denial of Service	Important	No	No	2
			CVE-2023-28250	Remote Code Execution	Critical	No	No	2
			CVE-2023-24925	Remote Code Execution	Important	No	No	2
			CVE-2023-24928	Remote Code Execution	Important	No	No	2
			CVE-2023-28247	Information Disclosure	Important	No	No	2
			CVE-2023-28241	Denial of Service	Important	No	No	2
			CVE-2023-28276	Security Feature Bypass	Important	No	No	2
			CVE-2023-28272	Elevation of Privilege	Important	No	No	2
			CVE-2023-28306	Remote Code Execution	Important	No	No	2
			CVE-2023-28269	Security Feature Bypass	Important	No	No	2
			CVE-2023-28231	Remote Code Execution	Critical	No	No	1
			CVE-2023-24887	Remote Code Execution	Important	No	No	2
			CVE-2023-28278	Remote Code Execution	Important	No	No	2

			CVE-2023-28307	Remote Code Execution	Important	No	No	2
			CVE-2023-28243	Remote Code Execution	Important	No	No	2
<a href="#">5025277</a>	高危	April 11, 2023—KB5025277 (Security-only update) – Microsoft Support for Windows Server 2008 R2 Enterprise ESU, Windows Server 2008 R2 Standard ESU, Windows Server 2008 R2 Datacenter ESU	CVE-2023-21729	Information Disclosure	Important	No	No	2
			CVE-2023-28253	Information Disclosure	Important	No	No	2
			CVE-2023-28220	Remote Code Execution	Critical	No	No	1
			CVE-2023-28229	Elevation of Privilege	Important	No	No	2
			CVE-2023-28252	Elevation of Privilege	Important	No	Yes	0
			CVE-2023-28218	Elevation of Privilege	Important	No	No	1
			CVE-2023-28293	Elevation of Privilege	Important	No	No	2
			CVE-2023-28266	Information Disclosure	Important	No	No	1
			CVE-2023-28308	Remote Code Execution	Important	No	No	2
			CVE-2023-28240	Remote Code Execution	Important	No	No	2
			CVE-2023-28217	Denial of Service	Important	No	No	2
			CVE-2023-28227	Remote Code Execution	Important	No	No	1
			CVE-2023-24931	Denial of Service	Important	No	No	2
			CVE-2023-28298	Denial of Service	Important	No	No	2
			CVE-2023-21554	Remote Code Execution	Critical	No	No	1
			CVE-2023-28256	Remote Code Execution	Important	No	No	2
			CVE-2023-28216	Elevation of Privilege	Important	No	No	2
			CVE-2023-28302	Denial of Service	Important	No	No	2

			CVE-2023-28271	Information Disclosure	Important	No	No	2
			CVE-2023-28228	Spoofing	Important	No	No	2
			CVE-2023-28275	Remote Code Execution	Important	No	No	2
			CVE-2023-28255	Remote Code Execution	Important	No	No	2
			CVE-2023-28223	Remote Code Execution	Important	No	No	2
			CVE-2023-28305	Remote Code Execution	Important	No	No	2
			CVE-2023-24912	Elevation of Privilege	Important	No	No	1
			CVE-2023-21727	Remote Code Execution	Important	No	No	2
			CVE-2023-28219	Remote Code Execution	Critical	No	No	1
			CVE-2023-28232	Remote Code Execution	Critical	No	No	2
			CVE-2023-28254	Remote Code Execution	Important	No	No	2
			CVE-2023-28268	Elevation of Privilege	Important	No	No	2
			CVE-2023-28238	Remote Code Execution	Important	No	No	2
			CVE-2023-28222	Elevation of Privilege	Important	No	No	2
			CVE-2023-28267	Information Disclosure	Important	No	No	2
			CVE-2023-28244	Elevation of Privilege	Important	No	No	2
			CVE-2023-21769	Denial of Service	Important	No	No	2
			CVE-2023-28250	Remote Code Execution	Critical	No	No	2
			CVE-2023-28241	Denial of Service	Important	No	No	2
			CVE-2023-28276	Security Feature Bypass	Important	No	No	2

			CVE-2023-28272	Elevation of Privilege	Important	No	No	2
			CVE-2023-28306	Remote Code Execution	Important	No	No	2
			CVE-2023-28231	Remote Code Execution	Critical	No	No	1
			CVE-2023-28278	Remote Code Execution	Important	No	No	2
			CVE-2023-28307	Remote Code Execution	Important	No	No	2
<a href="#">5025273</a>	高危	April 11, 2023—KB5025273 (Security-only update) – Microsoft Support for Windows Server 2008 Datacenter ESU, Windows Server 2008 Standard ESU, Windows Server 2008 Enterprise ESU	CVE-2023-21729	Information Disclosure	Important	No	No	2
			CVE-2023-28253	Information Disclosure	Important	No	No	2
			CVE-2023-28220	Remote Code Execution	Critical	No	No	1
			CVE-2023-28229	Elevation of Privilege	Important	No	No	2
			CVE-2023-28252	Elevation of Privilege	Important	No	Yes	0
			CVE-2023-28218	Elevation of Privilege	Important	No	No	1
			CVE-2023-28293	Elevation of Privilege	Important	No	No	2
			CVE-2023-28266	Information Disclosure	Important	No	No	1
			CVE-2023-28308	Remote Code Execution	Important	No	No	2
			CVE-2023-28240	Remote Code Execution	Important	No	No	2
			CVE-2023-28217	Denial of Service	Important	No	No	2
			CVE-2023-28227	Remote Code Execution	Important	No	No	1
			CVE-2023-28298	Denial of Service	Important	No	No	2
			CVE-2023-21554	Remote Code Execution	Critical	No	No	1
			CVE-2023-28256	Remote Code Execution	Important	No	No	2

			CVE-2023-28216	Elevation of Privilege	Important	No	No	2
			CVE-2023-28302	Denial of Service	Important	No	No	2
			CVE-2023-28271	Information Disclosure	Important	No	No	2
			CVE-2023-28228	Spoofing	Important	No	No	2
			CVE-2023-28275	Remote Code Execution	Important	No	No	2
			CVE-2023-28255	Remote Code Execution	Important	No	No	2
			CVE-2023-28223	Remote Code Execution	Important	No	No	2
			CVE-2023-28305	Remote Code Execution	Important	No	No	2
			CVE-2023-24912	Elevation of Privilege	Important	No	No	1
			CVE-2023-21727	Remote Code Execution	Important	No	No	2
			CVE-2023-28219	Remote Code Execution	Critical	No	No	1
			CVE-2023-28232	Remote Code Execution	Critical	No	No	2
			CVE-2023-28254	Remote Code Execution	Important	No	No	2
			CVE-2023-28268	Elevation of Privilege	Important	No	No	2
			CVE-2023-28222	Elevation of Privilege	Important	No	No	2
			CVE-2023-28244	Elevation of Privilege	Important	No	No	2
			CVE-2023-21769	Denial of Service	Important	No	No	2
			CVE-2023-28250	Remote Code Execution	Critical	No	No	2
			CVE-2023-28241	Denial of Service	Important	No	No	2
			CVE-2023-28276	Security Feature Bypass	Important	No	No	2



			CVE-2023-28272	Elevation of Privilege	Important	No	No	2
			CVE-2023-28306	Remote Code Execution	Important	No	No	2
			CVE-2023-28231	Remote Code Execution	Critical	No	No	1
			CVE-2023-28278	Remote Code Execution	Important	No	No	2
			CVE-2023-28307	Remote Code Execution	Important	No	No	2
<a href="#">5025221</a>	高危	April 11, 2023—KB5025221 (OS Builds 19042.2846, 19044.2846, and 19045.2846) – Microsoft Support for Windows 10 Enterprise Multi-Session, version 20H2, Windows 10 Enterprise and Education, version	CVE-2023-21729	Information Disclosure	Important	No	No	2
			CVE-2023-28253	Information Disclosure	Important	No	No	2
			CVE-2023-28220	Remote Code Execution	Critical	No	No	1
			CVE-2023-28273	Elevation of Privilege	Important	No	No	2
			CVE-2023-28229	Elevation of Privilege	Important	No	No	2
			CVE-2023-28252	Elevation of Privilege	Important	No	Yes	0
			CVE-2023-24886	Remote Code Execution	Important	No	No	2
			CVE-2023-24927	Remote Code Execution	Important	No	No	2
			CVE-2023-24924	Remote Code Execution	Important	No	No	2
			CVE-2023-28218	Elevation of Privilege	Important	No	No	1
			CVE-2023-28293	Elevation of Privilege	Important	No	No	2
			CVE-2023-28266	Information Disclosure	Important	No	No	1
			CVE-2023-28236	Elevation of Privilege	Important	No	No	2
			CVE-2023-28217	Denial of Service	Important	No	No	2
			CVE-2023-28227	Remote Code Execution	Important	No	No	1

	20H2, Windows 10 IoT Enterprise, version 20H2, Windows 10 on Surface Hub, Windows 10, version 21H2, all editions, Windows 10, version 22H2, all editions	CVE-2023-28235	Security Feature Bypass	Important	No	No	2
		CVE-2023-24931	Denial of Service	Important	No	No	2
		CVE-2023-28298	Denial of Service	Important	No	No	2
		CVE-2023-21554	Remote Code Execution	Critical	No	No	1
		CVE-2023-28216	Elevation of Privilege	Important	No	No	2
		CVE-2023-28249	Security Feature Bypass	Important	No	No	2
		CVE-2023-28302	Denial of Service	Important	No	No	2
		CVE-2023-28271	Information Disclosure	Important	No	No	2
		CVE-2023-28228	Spoofing	Important	No	No	2
		CVE-2023-28275	Remote Code Execution	Important	No	No	2
		CVE-2023-24885	Remote Code Execution	Important	No	No	2
		CVE-2023-28225	Elevation of Privilege	Important	No	No	2
		CVE-2023-28248	Elevation of Privilege	Important	No	No	2
		CVE-2023-28226	Security Feature Bypass	Important	No	No	2
		CVE-2023-28270	Security Feature Bypass	Important	No	No	2
		CVE-2023-24883	Information Disclosure	Important	No	No	2
		CVE-2023-24912	Elevation of Privilege	Important	No	No	1
		CVE-2023-21727	Remote Code Execution	Important	No	No	2
		CVE-2023-28219	Remote Code Execution	Critical	No	No	1

			CVE-2023-28274	Elevation of Privilege	Important	No	No	1
			CVE-2023-28224	Remote Code Execution	Important	No	No	2
			CVE-2023-28232	Remote Code Execution	Critical	No	No	2
			CVE-2023-24884	Remote Code Execution	Important	No	No	2
			CVE-2023-28238	Remote Code Execution	Important	No	No	2
			CVE-2023-28222	Elevation of Privilege	Important	No	No	2
			CVE-2023-24929	Remote Code Execution	Important	No	No	2
			CVE-2023-28267	Information Disclosure	Important	No	No	2
			CVE-2023-24926	Remote Code Execution	Important	No	No	2
			CVE-2023-28237	Remote Code Execution	Important	No	No	2
			CVE-2023-21769	Denial of Service	Important	No	No	2
			CVE-2023-28250	Remote Code Execution	Critical	No	No	2
			CVE-2023-24925	Remote Code Execution	Important	No	No	2
			CVE-2023-24928	Remote Code Execution	Important	No	No	2
			CVE-2023-28241	Denial of Service	Important	No	No	2
			CVE-2023-28276	Security Feature Bypass	Important	No	No	2
			CVE-2023-28272	Elevation of Privilege	Important	No	No	2
			CVE-2023-28269	Security Feature Bypass	Important	No	No	2
			CVE-2023-24887	Remote Code Execution	Important	No	No	2

			CVE-2023-28243	Remote Code Execution	Important	No	No	2
			CVE-2023-28221	Elevation of Privilege	Important	No	No	2
<a href="#">5025239</a>	高危	April 11, 2023—KB5025239 (OS Build 22621.1555) – Microsoft Support for Windows 11 version 22H2, all editions	CVE-2023-21729	Information Disclosure	Important	No	No	2
			CVE-2023-28253	Information Disclosure	Important	No	No	2
			CVE-2023-28220	Remote Code Execution	Critical	No	No	1
			CVE-2023-28273	Elevation of Privilege	Important	No	No	2
			CVE-2023-28229	Elevation of Privilege	Important	No	No	2
			CVE-2023-28252	Elevation of Privilege	Important	No	Yes	0
			CVE-2023-24886	Remote Code Execution	Important	No	No	2
			CVE-2023-24927	Remote Code Execution	Important	No	No	2
			CVE-2023-24924	Remote Code Execution	Important	No	No	2
			CVE-2023-28218	Elevation of Privilege	Important	No	No	1
			CVE-2023-28293	Elevation of Privilege	Important	No	No	2
			CVE-2023-28266	Information Disclosure	Important	No	No	1
			CVE-2023-28236	Elevation of Privilege	Important	No	No	2
			CVE-2023-28217	Denial of Service	Important	No	No	2
			CVE-2023-28227	Remote Code Execution	Important	No	No	1
			CVE-2023-24931	Denial of Service	Important	No	No	2
			CVE-2023-28233	Denial of Service	Important	No	No	2
			CVE-2023-28298	Denial of Service	Important	No	No	2

			CVE-2023-21554	Remote Code Execution	Critical	No	No	1
			CVE-2023-28216	Elevation of Privilege	Important	No	No	2
			CVE-2023-28249	Security Feature Bypass	Important	No	No	2
			CVE-2023-28302	Denial of Service	Important	No	No	2
			CVE-2023-28271	Information Disclosure	Important	No	No	2
			CVE-2023-28228	Spoofing	Important	No	No	2
			CVE-2023-28275	Remote Code Execution	Important	No	No	2
			CVE-2023-24885	Remote Code Execution	Important	No	No	2
			CVE-2023-28234	Denial of Service	Important	No	No	2
			CVE-2023-28225	Elevation of Privilege	Important	No	No	2
			CVE-2023-28248	Elevation of Privilege	Important	No	No	2
			CVE-2023-28226	Security Feature Bypass	Important	No	No	2
			CVE-2023-28270	Security Feature Bypass	Important	No	No	2
			CVE-2023-24914	Elevation of Privilege	Important	No	No	2
			CVE-2023-24883	Information Disclosure	Important	No	No	2
			CVE-2023-24912	Elevation of Privilege	Important	No	No	1
			CVE-2023-21727	Remote Code Execution	Important	No	No	2
			CVE-2023-28219	Remote Code Execution	Critical	No	No	1
			CVE-2023-28274	Elevation of Privilege	Important	No	No	1

			CVE-2023-28224	Remote Code Execution	Important	No	No	2
			CVE-2023-28232	Remote Code Execution	Critical	No	No	2
			CVE-2023-24884	Remote Code Execution	Important	No	No	2
			CVE-2023-28238	Remote Code Execution	Important	No	No	2
			CVE-2023-28222	Elevation of Privilege	Important	No	No	2
			CVE-2023-24929	Remote Code Execution	Important	No	No	2
			CVE-2023-28267	Information Disclosure	Important	No	No	2
			CVE-2023-24926	Remote Code Execution	Important	No	No	2
			CVE-2023-28237	Remote Code Execution	Important	No	No	2
			CVE-2023-21769	Denial of Service	Important	No	No	2
			CVE-2023-28250	Remote Code Execution	Critical	No	No	2
			CVE-2023-24925	Remote Code Execution	Important	No	No	2
			CVE-2023-24928	Remote Code Execution	Important	No	No	2
			CVE-2023-28241	Denial of Service	Important	No	No	2
			CVE-2023-28276	Security Feature Bypass	Important	No	No	2
			CVE-2023-28272	Elevation of Privilege	Important	No	No	2
			CVE-2023-28246	Elevation of Privilege	Important	No	No	2
			CVE-2023-28269	Security Feature Bypass	Important	No	No	2
			CVE-2023-24887	Remote Code Execution	Important	No	No	2

			CVE-2023-28243	Remote Code Execution	Important	No	No	2
			CVE-2023-28221	Elevation of Privilege	Important	No	No	2
<a href="#">5025228</a>	高危	April 11, 2023—KB5025228 (OS Build 14393.5850) – Microsoft Support for Windows 10, version 1607, all editions, Windows Server 2016, all editions	CVE-2023-21729	Information Disclosure	Important	No	No	2
			CVE-2023-28253	Information Disclosure	Important	No	No	2
			CVE-2023-28220	Remote Code Execution	Critical	No	No	1
			CVE-2023-28273	Elevation of Privilege	Important	No	No	2
			CVE-2023-28229	Elevation of Privilege	Important	No	No	2
			CVE-2023-28252	Elevation of Privilege	Important	No	Yes	0
			CVE-2023-24886	Remote Code Execution	Important	No	No	2
			CVE-2023-24927	Remote Code Execution	Important	No	No	2
			CVE-2023-24924	Remote Code Execution	Important	No	No	2
			CVE-2023-28218	Elevation of Privilege	Important	No	No	1
			CVE-2023-28293	Elevation of Privilege	Important	No	No	2
			CVE-2023-28266	Information Disclosure	Important	No	No	1
			CVE-2023-28308	Remote Code Execution	Important	No	No	2
			CVE-2023-28240	Remote Code Execution	Important	No	No	2
			CVE-2023-28236	Elevation of Privilege	Important	No	No	2
			CVE-2023-28217	Denial of Service	Important	No	No	2
			CVE-2023-28227	Remote Code Execution	Important	No	No	1
			CVE-2023-24931	Denial of Service	Important	No	No	2

			CVE-2023-28298	Denial of Service	Important	No	No	2
			CVE-2023-21554	Remote Code Execution	Critical	No	No	1
			CVE-2023-28256	Remote Code Execution	Important	No	No	2
			CVE-2023-28216	Elevation of Privilege	Important	No	No	2
			CVE-2023-28249	Security Feature Bypass	Important	No	No	2
			CVE-2023-28302	Denial of Service	Important	No	No	2
			CVE-2023-28271	Information Disclosure	Important	No	No	2
			CVE-2023-28228	Spoofing	Important	No	No	2
			CVE-2023-28275	Remote Code Execution	Important	No	No	2
			CVE-2023-28255	Remote Code Execution	Important	No	No	2
			CVE-2023-28223	Remote Code Execution	Important	No	No	2
			CVE-2023-24885	Remote Code Execution	Important	No	No	2
			CVE-2023-28225	Elevation of Privilege	Important	No	No	2
			CVE-2023-28248	Elevation of Privilege	Important	No	No	2
			CVE-2023-28226	Security Feature Bypass	Important	No	No	2
			CVE-2023-28305	Remote Code Execution	Important	No	No	2
			CVE-2023-24883	Information Disclosure	Important	No	No	2
			CVE-2023-24912	Elevation of Privilege	Important	No	No	1
			CVE-2023-21727	Remote Code Execution	Important	No	No	2
			CVE-2023-28219	Remote Code Execution	Critical	No	No	1



			CVE-2023-28224	Remote Code Execution	Important	No	No	2
			CVE-2023-28232	Remote Code Execution	Critical	No	No	2
			CVE-2023-28254	Remote Code Execution	Important	No	No	2
			CVE-2023-24884	Remote Code Execution	Important	No	No	2
			CVE-2023-28268	Elevation of Privilege	Important	No	No	2
			CVE-2023-28238	Remote Code Execution	Important	No	No	2
			CVE-2023-28222	Elevation of Privilege	Important	No	No	2
			CVE-2023-24929	Remote Code Execution	Important	No	No	2
			CVE-2023-28267	Information Disclosure	Important	No	No	2
			CVE-2023-24926	Remote Code Execution	Important	No	No	2
			CVE-2023-28244	Elevation of Privilege	Important	No	No	2
			CVE-2023-28237	Remote Code Execution	Important	No	No	2
			CVE-2023-21769	Denial of Service	Important	No	No	2
			CVE-2023-28250	Remote Code Execution	Critical	No	No	2
			CVE-2023-24925	Remote Code Execution	Important	No	No	2
			CVE-2023-24928	Remote Code Execution	Important	No	No	2
			CVE-2023-28247	Information Disclosure	Important	No	No	2
			CVE-2023-28241	Denial of Service	Important	No	No	2
			CVE-2023-28276	Security Feature Bypass	Important	No	No	2
			CVE-2023-28272	Elevation of Privilege	Important	No	No	2

			CVE-2023-28306	Remote Code Execution	Important	No	No	2
			CVE-2023-28269	Security Feature Bypass	Important	No	No	2
			CVE-2023-28231	Remote Code Execution	Critical	No	No	1
			CVE-2023-24887	Remote Code Execution	Important	No	No	2
			CVE-2023-28278	Remote Code Execution	Important	No	No	2
			CVE-2023-28307	Remote Code Execution	Important	No	No	2
			CVE-2023-28243	Remote Code Execution	Important	No	No	2
			CVE-2023-28221	Elevation of Privilege	Important	No	No	2
<a href="#">5025287</a>	高危	April 11, 2023—KB5025287 (Monthly Rollup) - Microsoft Support for Windows Server 2012, Windows Embedded 8 Standard	CVE-2023-21729	Information Disclosure	Important	No	No	2
			CVE-2023-28253	Information Disclosure	Important	No	No	2
			CVE-2023-28220	Remote Code Execution	Critical	No	No	1
			CVE-2023-28229	Elevation of Privilege	Important	No	No	2
			CVE-2023-28252	Elevation of Privilege	Important	No	Yes	0
			CVE-2023-24886	Remote Code Execution	Important	No	No	2
			CVE-2023-24927	Remote Code Execution	Important	No	No	2
			CVE-2023-24924	Remote Code Execution	Important	No	No	2
			CVE-2023-28218	Elevation of Privilege	Important	No	No	1
			CVE-2023-28293	Elevation of Privilege	Important	No	No	2
			CVE-2023-28266	Information Disclosure	Important	No	No	1
			CVE-2023-28308	Remote Code Execution	Important	No	No	2

			CVE-2023-28240	Remote Code Execution	Important	No	No	2
			CVE-2023-28236	Elevation of Privilege	Important	No	No	2
			CVE-2023-28217	Denial of Service	Important	No	No	2
			CVE-2023-28227	Remote Code Execution	Important	No	No	1
			CVE-2023-24931	Denial of Service	Important	No	No	2
			CVE-2023-28298	Denial of Service	Important	No	No	2
			CVE-2023-21554	Remote Code Execution	Critical	No	No	1
			CVE-2023-28256	Remote Code Execution	Important	No	No	2
			CVE-2023-28216	Elevation of Privilege	Important	No	No	2
			CVE-2023-28249	Security Feature Bypass	Important	No	No	2
			CVE-2023-28302	Denial of Service	Important	No	No	2
			CVE-2023-28271	Information Disclosure	Important	No	No	2
			CVE-2023-28228	Spoofing	Important	No	No	2
			CVE-2023-28275	Remote Code Execution	Important	No	No	2
			CVE-2023-28255	Remote Code Execution	Important	No	No	2
			CVE-2023-28223	Remote Code Execution	Important	No	No	2
			CVE-2023-24885	Remote Code Execution	Important	No	No	2
			CVE-2023-28305	Remote Code Execution	Important	No	No	2
			CVE-2023-24883	Information Disclosure	Important	No	No	2
			CVE-2023-24912	Elevation of Privilege	Important	No	No	1

			CVE-2023-21727	Remote Code Execution	Important	No	No	2
			CVE-2023-28219	Remote Code Execution	Critical	No	No	1
			CVE-2023-28224	Remote Code Execution	Important	No	No	2
			CVE-2023-28232	Remote Code Execution	Critical	No	No	2
			CVE-2023-28254	Remote Code Execution	Important	No	No	2
			CVE-2023-24884	Remote Code Execution	Important	No	No	2
			CVE-2023-28268	Elevation of Privilege	Important	No	No	2
			CVE-2023-28238	Remote Code Execution	Important	No	No	2
			CVE-2023-28222	Elevation of Privilege	Important	No	No	2
			CVE-2023-24929	Remote Code Execution	Important	No	No	2
			CVE-2023-28267	Information Disclosure	Important	No	No	2
			CVE-2023-24926	Remote Code Execution	Important	No	No	2
			CVE-2023-28244	Elevation of Privilege	Important	No	No	2
			CVE-2023-28237	Remote Code Execution	Important	No	No	2
			CVE-2023-21769	Denial of Service	Important	No	No	2
			CVE-2023-28250	Remote Code Execution	Critical	No	No	2
			CVE-2023-24925	Remote Code Execution	Important	No	No	2
			CVE-2023-24928	Remote Code Execution	Important	No	No	2
			CVE-2023-28247	Information Disclosure	Important	No	No	2
			CVE-2023-28241	Denial of Service	Important	No	No	2

			CVE-2023-28276	Security Feature Bypass	Important	No	No	2
			CVE-2023-28272	Elevation of Privilege	Important	No	No	2
			CVE-2023-28306	Remote Code Execution	Important	No	No	2
			CVE-2023-28269	Security Feature Bypass	Important	No	No	2
			CVE-2023-28231	Remote Code Execution	Critical	No	No	1
			CVE-2023-24887	Remote Code Execution	Important	No	No	2
			CVE-2023-28278	Remote Code Execution	Important	No	No	2
			CVE-2023-28307	Remote Code Execution	Important	No	No	2
			CVE-2023-28243	Remote Code Execution	Important	No	No	2

本月微软发布的软件安全更新补丁共 4 个，详细列表如下：

KBID	奇安信集团级别	补丁名称	修复的漏洞	漏洞的影响	漏洞等级	公开披露	已受攻击	漏洞的可利用性
<a href="#">5002383</a>	高危	Description of the security update for SharePoint Foundation 2013: April 11, 2023 (KB500238	CVE-2023-28288	Spoofing	Important	No	No	2

		3) - Microsoft Support						
<a href="#">5002221</a>	高危	Description of the security update for Publisher 2016: April 11, 2023 (KB5002221) - Microsoft Support	CVE-2023-28295	Remote Code Execution	Important	No	No	2
			CVE-2023-28287	Remote Code Execution	Important	No	No	2
<a href="#">5002385</a>	高危	Description of the security update for SharePoint Enterprise Server 2016: April 11, 2023 (KB5002385) - Microsoft Support	CVE-2023-28288	Spoofing	Important	No	No	2
<a href="#">5002213</a>	高危	Description of the security update for Publisher 2013: April 11, 2023 (KB5002213) - Microsoft Support	CVE-2023-28295	Remote Code Execution	Important	No	No	2
			CVE-2023-28287	Remote Code Execution	Important	No	No	2

		3) - Microsoft Support						
--	--	------------------------------	--	--	--	--	--	--

本月发布内容无一般性更新补丁。

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>