

奇安信集团 2023 年 3 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 3 月 15 日

目 录

第 1 章 安全通告.....	2
第 2 章 重点关注补丁.....	3
第 3 章 已知问题和特殊调整.....	7
第 4 章 漏洞补丁详细列表.....	8
第 5 章 参考链接.....	39

文档信息

文档名称	奇安信集团 2023 年 3 月补丁库更新通告		
文档编号	Qi An Xin Group-MSPatch-2023-0301		
发布日期	2023-03-15	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:2023.03.15.1,V10 版本:2023.03.15.1000)已发布,本次更新推送了 24 个微软安全补丁,修复了 61 个安全漏洞,其中 9 个微软官方评级为“严重(Critical)”,52 个评级为“重要(Important)”,这些漏洞影响产品 Windows、Microsoft Office。

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
5002348	CVE-2023-23398	Spoofing	Important	No	No	Exploitation More Likely
5002351						
5023696	CVE-2023-1018	Elevation of Privilege	Critical	No	No	Exploitation Less Likely
5023702						
5023697						
5023698						
5023706						
5023713						
5023696	CVE-2023-23410	Elevation of Privilege	Important	No	No	Exploitation More Likely
5023702						
5023697						
5023764						
5023756						
5023698						
5023755						
5023706						
5023713						
5023759						
5023769						
5023765						
5023752						
5023754						
5023696	CVE-2023-23411	Denial of Service	Critical	No	No	Exploitation Less Likely
5023702						
5023697						
5023698						

5023706						
5023713						
5023696	CVE-2023-21708	Remote Code Execution	Critical	No	No	Exploitation Less Likely
5023702						
5023697						
5023764						
5023756						
5023698						
5023755						
5023706						
5023713						
5023759						
5023769						
5023765						
5023752						
5023754						
5023696	CVE-2023-23404	Remote Code Execution	Critical	No	No	Exploitation Less Likely
5023702						
5023697						
5023764						
5023756						
5023698						
5023706						
5023713						
5023765						
5023752						
5023696	CVE-2023-1017	Elevation of Privilege	Critical	No	No	Exploitation Less Likely
5023702						
5023697						
5023698						
5023706						
5023713						
5023696	CVE-2023-24861	Elevation of Privilege	Important	No	No	Exploitation More Likely
5023702						
5023697						
5023764						
5023756						
5023698						

5023755						
5023706						
5023713						
5023759						
5023769						
5023765						
5023752						
5023754						
5023696	CVE-2023-23415	Remote Code Execution	Critical	No	No	Exploitation More Likely
5023702						
5023697						
5023764						
5023756						
5023698						
5023755						
5023706						
5023713						
5023759						
5023769						
5023765						
5023752						
5023754						
5023696	CVE-2023-24880	Security Feature Bypass	Moderate	Yes	Yes	Exploitation Detected
5023702						
5023697						
5023698						
5023706						
5023696	CVE-2023-23416	Remote Code Execution	Critical	No	No	Exploitation More Likely
5023702						
5023697						
5023764						
5023756						
5023698						
5023706						
5023713						
5023765						
5023752						

5023698	CVE-2023-23392	Remote Code Execution	Critical	No	No	Exploitation More Likely
5023706						
5002254	CVE-2023-23397	Elevation of Privilege	Critical	No	Yes	Exploitation Detected
5002265						

第3章 已知问题和特殊调整

本月暂无已知问题和特殊调整。

第4章 漏洞补丁详细列表

本月微软发布的系统安全更新补丁共 14 个，详细列表如下：

KBID	奇安信集团级别	补丁名称	CVE 漏洞	漏洞的影响	漏洞等级	公开披露	已受攻击	漏洞的可利用性
5023696	高危	March 14, 2023—KB5023696 (OS Builds 19042. 2728, 19044. 2728, and 19045. 2728) – Microsoft Support for Windows 10 Enterprise Multi-Session, version 20H2, Windows 10 Enterprise and Education, version 20H2, Windows 10 IoT Enterprise, version 20H2, Windo	CVE-2023-23394	Information Disclosure	Important	No	No	2
			CVE-2023-1018	Elevation of Privilege	Critical	No	No	2
			CVE-2023-23402	Remote Code Execution	Important	No	No	2
			CVE-2023-24870	Information Disclosure	Important	No	No	2
			CVE-2023-24910	Elevation of Privilege	Important	No	No	2
			CVE-2023-23409	Information Disclosure	Important	No	No	2
			CVE-2023-23410	Elevation of Privilege	Important	No	No	1
			CVE-2023-23417	Elevation of Privilege	Important	No	No	2
			CVE-2023-24866	Information Disclosure	Important	No	No	2
			CVE-2023-23422	Elevation of Privilege	Important	No	No	2
			CVE-2023-24858	Information Disclosure	Important	No	No	2
			CVE-2023-23423	Elevation of Privilege	Important	No	No	2
			CVE-2023-23414	Remote Code Execution	Important	No	No	2
			CVE-2023-24868	Remote Code Execution	Important	No	No	2

ws 10 on Surface Hub, Windows 10, version 21H2, all editions, Windows 10, version 22H2, all editions	CVE-2023-23411	Denial of Service	Critical	No	No	2
	CVE-2023-24907	Remote Code Execution	Important	No	No	2
	CVE-2023-21708	Remote Code Execution	Critical	No	No	2
	CVE-2023-23421	Elevation of Privilege	Important	No	No	2
	CVE-2023-24862	Denial of Service	Important	No	No	2
	CVE-2023-23407	Remote Code Execution	Important	No	No	2
	CVE-2023-24869	Remote Code Execution	Important	No	No	2
	CVE-2023-23404	Remote Code Execution	Critical	No	No	2
	CVE-2023-24913	Remote Code Execution	Important	No	No	2
	CVE-2023-23413	Remote Code Execution	Important	No	No	2
	CVE-2023-23405	Remote Code Execution	Important	No	No	2
	CVE-2023-23420	Elevation of Privilege	Important	No	No	2
	CVE-2023-23401	Remote Code Execution	Important	No	No	2
	CVE-2023-24857	Information Disclosure	Important	No	No	2
	CVE-2023-24863	Information Disclosure	Important	No	No	2
	CVE-2023-24911	Information Disclosure	Important	No	No	2
	CVE-2023-1017	Elevation of Privilege	Critical	No	No	2
	CVE-2023-24861	Elevation of Privilege	Important	No	No	1
	CVE-2023-23403	Remote Code Execution	Important	No	No	2
	CVE-2023-23385	Elevation of Privilege	Important	No	No	2

			CVE-2023-24872	Remote Code Execution	Important	No	No	2
			CVE-2023-24876	Remote Code Execution	Important	No	No	2
			CVE-2023-24867	Remote Code Execution	Important	No	No	2
			CVE-2023-24906	Information Disclosure	Important	No	No	2
			CVE-2023-24908	Remote Code Execution	Important	No	No	2
			CVE-2023-23415	Remote Code Execution	Critical	No	No	1
			CVE-2023-23388	Elevation of Privilege	Important	No	No	2
			CVE-2023-24859	Denial of Service	Important	No	No	2
			CVE-2023-24856	Information Disclosure	Important	No	No	2
			CVE-2023-23406	Remote Code Execution	Important	No	No	2
			CVE-2023-24864	Elevation of Privilege	Important	No	No	2
			CVE-2023-23412	Elevation of Privilege	Important	No	No	2
			CVE-2023-24871	Remote Code Execution	Important	No	No	2
			CVE-2023-24865	Information Disclosure	Important	No	No	2
			CVE-2023-24909	Remote Code Execution	Important	No	No	2
			CVE-2023-24880	Security Feature Bypass	Moderate	Yes	Yes	0
			CVE-2023-23393	Elevation of Privilege	Important	No	No	2
			CVE-2023-23416	Remote Code Execution	Critical	No	No	1
5023702	高危	March 14, 2023— KB5023702 (OS Build	CVE-2023-23394	Information Disclosure	Important	No	No	2
			CVE-2023-1018	Elevation of Privilege	Critical	No	No	2

	17763.4131) - Microsoft Support for Win 10 Ent LTSC v2019, Win 10 IoT Ent LTSC v2019, Wind ows 10 IoT Core 2019 LTSC, Windo ws Server 2019	CVE-2023-23402	Remote Code Execution	Important	No	No	2
		CVE-2023-24870	Information Disclosure	Important	No	No	2
		CVE-2023-24910	Elevation of Privilege	Important	No	No	2
		CVE-2023-23409	Information Disclosure	Important	No	No	2
		CVE-2023-23410	Elevation of Privilege	Important	No	No	1
		CVE-2023-23417	Elevation of Privilege	Important	No	No	2
		CVE-2023-24866	Information Disclosure	Important	No	No	2
		CVE-2023-23422	Elevation of Privilege	Important	No	No	2
		CVE-2023-24858	Information Disclosure	Important	No	No	2
		CVE-2023-23423	Elevation of Privilege	Important	No	No	2
		CVE-2023-23414	Remote Code Execution	Important	No	No	2
		CVE-2023-24868	Remote Code Execution	Important	No	No	2
		CVE-2023-23411	Denial of Service	Critical	No	No	2
		CVE-2023-24907	Remote Code Execution	Important	No	No	2
		CVE-2023-21708	Remote Code Execution	Critical	No	No	2
		CVE-2023-23421	Elevation of Privilege	Important	No	No	2
		CVE-2023-24862	Denial of Service	Important	No	No	2
		CVE-2023-23407	Remote Code Execution	Important	No	No	2
		CVE-2023-24869	Remote Code Execution	Important	No	No	2
		CVE-2023-23404	Remote Code Execution	Critical	No	No	2

			CVE-2023-24913	Remote Code Execution	Important	No	No	2
			CVE-2023-23413	Remote Code Execution	Important	No	No	2
			CVE-2023-23405	Remote Code Execution	Important	No	No	2
			CVE-2023-23420	Elevation of Privilege	Important	No	No	2
			CVE-2023-23401	Remote Code Execution	Important	No	No	2
			CVE-2023-24857	Information Disclosure	Important	No	No	2
			CVE-2023-23400	Remote Code Execution	Important	No	No	2
			CVE-2023-24863	Information Disclosure	Important	No	No	2
			CVE-2023-24911	Information Disclosure	Important	No	No	2
			CVE-2023-1017	Elevation of Privilege	Critical	No	No	2
			CVE-2023-24861	Elevation of Privilege	Important	No	No	1
			CVE-2023-23403	Remote Code Execution	Important	No	No	2
			CVE-2023-23385	Elevation of Privilege	Important	No	No	2
			CVE-2023-24872	Remote Code Execution	Important	No	No	2
			CVE-2023-24876	Remote Code Execution	Important	No	No	2
			CVE-2023-24867	Remote Code Execution	Important	No	No	2
			CVE-2023-24906	Information Disclosure	Important	No	No	2
			CVE-2023-24908	Remote Code Execution	Important	No	No	2
			CVE-2023-23415	Remote Code Execution	Critical	No	No	1
			CVE-2023-23388	Elevation of Privilege	Important	No	No	2

			CVE-2023-24859	Denial of Service	Important	No	No	2
			CVE-2023-24856	Information Disclosure	Important	No	No	2
			CVE-2023-23406	Remote Code Execution	Important	No	No	2
			CVE-2023-24864	Elevation of Privilege	Important	No	No	2
			CVE-2023-23412	Elevation of Privilege	Important	No	No	2
			CVE-2023-24865	Information Disclosure	Important	No	No	2
			CVE-2023-24909	Remote Code Execution	Important	No	No	2
			CVE-2023-24880	Security Feature Bypass	Moderate	Yes	Yes	0
			CVE-2023-23393	Elevation of Privilege	Important	No	No	2
			CVE-2023-23416	Remote Code Execution	Critical	No	No	1
5023697	高危	March 14, 2023— KB5023697 (OS Build 14393.5786) – Microsoft Support for Windows 10, version 1607, all editions, Windows Server 2016, all editions	CVE-2023-23394	Information Disclosure	Important	No	No	2
			CVE-2023-1018	Elevation of Privilege	Critical	No	No	2
			CVE-2023-23402	Remote Code Execution	Important	No	No	2
			CVE-2023-24870	Information Disclosure	Important	No	No	2
			CVE-2023-24910	Elevation of Privilege	Important	No	No	2
			CVE-2023-23409	Information Disclosure	Important	No	No	2
			CVE-2023-23410	Elevation of Privilege	Important	No	No	1
			CVE-2023-23417	Elevation of Privilege	Important	No	No	2
			CVE-2023-24866	Information Disclosure	Important	No	No	2
			CVE-2023-23422	Elevation of Privilege	Important	No	No	2

			CVE-2023-24858	Information Disclosure	Important	No	No	2
			CVE-2023-23423	Elevation of Privilege	Important	No	No	2
			CVE-2023-23414	Remote Code Execution	Important	No	No	2
			CVE-2023-24868	Remote Code Execution	Important	No	No	2
			CVE-2023-23411	Denial of Service	Critical	No	No	2
			CVE-2023-24907	Remote Code Execution	Important	No	No	2
			CVE-2023-21708	Remote Code Execution	Critical	No	No	2
			CVE-2023-23421	Elevation of Privilege	Important	No	No	2
			CVE-2023-24862	Denial of Service	Important	No	No	2
			CVE-2023-23407	Remote Code Execution	Important	No	No	2
			CVE-2023-24869	Remote Code Execution	Important	No	No	2
			CVE-2023-23404	Remote Code Execution	Critical	No	No	2
			CVE-2023-24913	Remote Code Execution	Important	No	No	2
			CVE-2023-23413	Remote Code Execution	Important	No	No	2
			CVE-2023-23405	Remote Code Execution	Important	No	No	2
			CVE-2023-23420	Elevation of Privilege	Important	No	No	2
			CVE-2023-23401	Remote Code Execution	Important	No	No	2
			CVE-2023-24857	Information Disclosure	Important	No	No	2
			CVE-2023-23400	Remote Code Execution	Important	No	No	2
			CVE-2023-24863	Information Disclosure	Important	No	No	2

			CVE-2023-24911	Information Disclosure	Important	No	No	2
			CVE-2023-1017	Elevation of Privilege	Critical	No	No	2
			CVE-2023-24861	Elevation of Privilege	Important	No	No	1
			CVE-2023-23403	Remote Code Execution	Important	No	No	2
			CVE-2023-23385	Elevation of Privilege	Important	No	No	2
			CVE-2023-24872	Remote Code Execution	Important	No	No	2
			CVE-2023-24876	Remote Code Execution	Important	No	No	2
			CVE-2023-24867	Remote Code Execution	Important	No	No	2
			CVE-2023-24906	Information Disclosure	Important	No	No	2
			CVE-2023-24908	Remote Code Execution	Important	No	No	2
			CVE-2023-23415	Remote Code Execution	Critical	No	No	1
			CVE-2023-23388	Elevation of Privilege	Important	No	No	2
			CVE-2023-24859	Denial of Service	Important	No	No	2
			CVE-2023-24856	Information Disclosure	Important	No	No	2
			CVE-2023-23406	Remote Code Execution	Important	No	No	2
			CVE-2023-24864	Elevation of Privilege	Important	No	No	2
			CVE-2023-23412	Elevation of Privilege	Important	No	No	2
			CVE-2023-24865	Information Disclosure	Important	No	No	2
			CVE-2023-24909	Remote Code Execution	Important	No	No	2
			CVE-2023-24880	Security Feature Bypass	Moderate	Yes	Yes	0

			CVE-2023-23416	Remote Code Execution	Critical	No	No	1
5023764	高危	March 14, 2023—KB5023764 (Security-only update) - Microsoft Support for Windows Server 2012 R2, Windows Embedded 8.1 Industry Enterprise, Windows Embedded 8.1 Industry Pro	CVE-2023-23394	Information Disclosure	Important	No	No	2
			CVE-2023-23402	Remote Code Execution	Important	No	No	2
			CVE-2023-24870	Information Disclosure	Important	No	No	2
			CVE-2023-24910	Elevation of Privilege	Important	No	No	2
			CVE-2023-23409	Information Disclosure	Important	No	No	2
			CVE-2023-23410	Elevation of Privilege	Important	No	No	1
			CVE-2023-24866	Information Disclosure	Important	No	No	2
			CVE-2023-23422	Elevation of Privilege	Important	No	No	2
			CVE-2023-24858	Information Disclosure	Important	No	No	2
			CVE-2023-23423	Elevation of Privilege	Important	No	No	2
			CVE-2023-23414	Remote Code Execution	Important	No	No	2
			CVE-2023-24868	Remote Code Execution	Important	No	No	2
			CVE-2023-24907	Remote Code Execution	Important	No	No	2
			CVE-2023-21708	Remote Code Execution	Critical	No	No	2
			CVE-2023-23421	Elevation of Privilege	Important	No	No	2
			CVE-2023-24862	Denial of Service	Important	No	No	2
			CVE-2023-23407	Remote Code Execution	Important	No	No	2
CVE-2023-24869	Remote Code Execution	Important	No	No	2			
CVE-2023-23404	Remote Code Execution	Critical	No	No	2			

			CVE-2023-24913	Remote Code Execution	Important	No	No	2
			CVE-2023-23413	Remote Code Execution	Important	No	No	2
			CVE-2023-23405	Remote Code Execution	Important	No	No	2
			CVE-2023-23420	Elevation of Privilege	Important	No	No	2
			CVE-2023-23401	Remote Code Execution	Important	No	No	2
			CVE-2023-24857	Information Disclosure	Important	No	No	2
			CVE-2023-23400	Remote Code Execution	Important	No	No	2
			CVE-2023-24863	Information Disclosure	Important	No	No	2
			CVE-2023-24911	Information Disclosure	Important	No	No	2
			CVE-2023-24861	Elevation of Privilege	Important	No	No	1
			CVE-2023-23403	Remote Code Execution	Important	No	No	2
			CVE-2023-23385	Elevation of Privilege	Important	No	No	2
			CVE-2023-24876	Remote Code Execution	Important	No	No	2
			CVE-2023-24867	Remote Code Execution	Important	No	No	2
			CVE-2023-24906	Information Disclosure	Important	No	No	2
			CVE-2023-24908	Remote Code Execution	Important	No	No	2
			CVE-2023-23415	Remote Code Execution	Critical	No	No	1
			CVE-2023-24859	Denial of Service	Important	No	No	2
			CVE-2023-24856	Information Disclosure	Important	No	No	2
			CVE-2023-23406	Remote Code Execution	Important	No	No	2

			CVE-2023-24864	Elevation of Privilege	Important	No	No	2
			CVE-2023-23412	Elevation of Privilege	Important	No	No	2
			CVE-2023-24865	Information Disclosure	Important	No	No	2
			CVE-2023-24909	Remote Code Execution	Important	No	No	2
			CVE-2023-23416	Remote Code Execution	Critical	No	No	1
5023756	高危	March 14, 2023—KB5023756 (Monthly Rollup) – Microsoft Support for Windows Server 2012, Windows Embedded 8 Standard	CVE-2023-23394	Information Disclosure	Important	No	No	2
			CVE-2023-23402	Remote Code Execution	Important	No	No	2
			CVE-2023-24870	Information Disclosure	Important	No	No	2
			CVE-2023-24910	Elevation of Privilege	Important	No	No	2
			CVE-2023-23409	Information Disclosure	Important	No	No	2
			CVE-2023-23410	Elevation of Privilege	Important	No	No	1
			CVE-2023-24866	Information Disclosure	Important	No	No	2
			CVE-2023-23422	Elevation of Privilege	Important	No	No	2
			CVE-2023-24858	Information Disclosure	Important	No	No	2
			CVE-2023-23423	Elevation of Privilege	Important	No	No	2
			CVE-2023-23414	Remote Code Execution	Important	No	No	2
			CVE-2023-24868	Remote Code Execution	Important	No	No	2
			CVE-2023-24907	Remote Code Execution	Important	No	No	2
			CVE-2023-21708	Remote Code Execution	Critical	No	No	2
			CVE-2023-23421	Elevation of Privilege	Important	No	No	2

			CVE-2023-24862	Denial of Service	Important	No	No	2
			CVE-2023-23407	Remote Code Execution	Important	No	No	2
			CVE-2023-24869	Remote Code Execution	Important	No	No	2
			CVE-2023-23404	Remote Code Execution	Critical	No	No	2
			CVE-2023-24913	Remote Code Execution	Important	No	No	2
			CVE-2023-23413	Remote Code Execution	Important	No	No	2
			CVE-2023-23405	Remote Code Execution	Important	No	No	2
			CVE-2023-23420	Elevation of Privilege	Important	No	No	2
			CVE-2023-23401	Remote Code Execution	Important	No	No	2
			CVE-2023-24857	Information Disclosure	Important	No	No	2
			CVE-2023-24863	Information Disclosure	Important	No	No	2
			CVE-2023-24911	Information Disclosure	Important	No	No	2
			CVE-2023-24861	Elevation of Privilege	Important	No	No	1
			CVE-2023-23403	Remote Code Execution	Important	No	No	2
			CVE-2023-23385	Elevation of Privilege	Important	No	No	2
			CVE-2023-24872	Remote Code Execution	Important	No	No	2
			CVE-2023-24876	Remote Code Execution	Important	No	No	2
			CVE-2023-24867	Remote Code Execution	Important	No	No	2
			CVE-2023-24906	Information Disclosure	Important	No	No	2
			CVE-2023-24908	Remote Code Execution	Important	No	No	2

			CVE-2023-23415	Remote Code Execution	Critical	No	No	1
			CVE-2023-24859	Denial of Service	Important	No	No	2
			CVE-2023-24856	Information Disclosure	Important	No	No	2
			CVE-2023-23406	Remote Code Execution	Important	No	No	2
			CVE-2023-24864	Elevation of Privilege	Important	No	No	2
			CVE-2023-23412	Elevation of Privilege	Important	No	No	2
			CVE-2023-24865	Information Disclosure	Important	No	No	2
			CVE-2023-24909	Remote Code Execution	Important	No	No	2
			CVE-2023-23416	Remote Code Execution	Critical	No	No	1
5023698	高危	March 14, 2023—KB5023698 (OS Build 22000.1696) - Microsoft Support for Windows 11 version 21H2, all editions	CVE-2023-23394	Information Disclosure	Important	No	No	2
			CVE-2023-1018	Elevation of Privilege	Critical	No	No	2
			CVE-2023-23402	Remote Code Execution	Important	No	No	2
			CVE-2023-24870	Information Disclosure	Important	No	No	2
			CVE-2023-24910	Elevation of Privilege	Important	No	No	2
			CVE-2023-23409	Information Disclosure	Important	No	No	2
			CVE-2023-23410	Elevation of Privilege	Important	No	No	1
			CVE-2023-23417	Elevation of Privilege	Important	No	No	2
			CVE-2023-24866	Information Disclosure	Important	No	No	2
			CVE-2023-23422	Elevation of Privilege	Important	No	No	2
			CVE-2023-24858	Information Disclosure	Important	No	No	2

			CVE-2023-23423	Elevation of Privilege	Important	No	No	2
			CVE-2023-23414	Remote Code Execution	Important	No	No	2
			CVE-2023-24868	Remote Code Execution	Important	No	No	2
			CVE-2023-23411	Denial of Service	Critical	No	No	2
			CVE-2023-24907	Remote Code Execution	Important	No	No	2
			CVE-2023-21708	Remote Code Execution	Critical	No	No	2
			CVE-2023-23421	Elevation of Privilege	Important	No	No	2
			CVE-2023-24862	Denial of Service	Important	No	No	2
			CVE-2023-23407	Remote Code Execution	Important	No	No	2
			CVE-2023-23392	Remote Code Execution	Critical	No	No	1
			CVE-2023-24869	Remote Code Execution	Important	No	No	2
			CVE-2023-23404	Remote Code Execution	Critical	No	No	2
			CVE-2023-24913	Remote Code Execution	Important	No	No	2
			CVE-2023-23413	Remote Code Execution	Important	No	No	2
			CVE-2023-23405	Remote Code Execution	Important	No	No	2
			CVE-2023-23420	Elevation of Privilege	Important	No	No	2
			CVE-2023-23401	Remote Code Execution	Important	No	No	2
			CVE-2023-24857	Information Disclosure	Important	No	No	2
			CVE-2023-24863	Information Disclosure	Important	No	No	2
			CVE-2023-24911	Information Disclosure	Important	No	No	2

			CVE-2023-1017	Elevation of Privilege	Critical	No	No	2
			CVE-2023-24861	Elevation of Privilege	Important	No	No	1
			CVE-2023-23403	Remote Code Execution	Important	No	No	2
			CVE-2023-23385	Elevation of Privilege	Important	No	No	2
			CVE-2023-24872	Remote Code Execution	Important	No	No	2
			CVE-2023-24876	Remote Code Execution	Important	No	No	2
			CVE-2023-24867	Remote Code Execution	Important	No	No	2
			CVE-2023-24906	Information Disclosure	Important	No	No	2
			CVE-2023-24908	Remote Code Execution	Important	No	No	2
			CVE-2023-23415	Remote Code Execution	Critical	No	No	1
			CVE-2023-23388	Elevation of Privilege	Important	No	No	2
			CVE-2023-24859	Denial of Service	Important	No	No	2
			CVE-2023-24856	Information Disclosure	Important	No	No	2
			CVE-2023-23406	Remote Code Execution	Important	No	No	2
			CVE-2023-24864	Elevation of Privilege	Important	No	No	2
			CVE-2023-24871	Remote Code Execution	Important	No	No	2
			CVE-2023-24865	Information Disclosure	Important	No	No	2
			CVE-2023-24909	Remote Code Execution	Important	No	No	2
			CVE-2023-24880	Security Feature Bypass	Moderate	Yes	Yes	0
			CVE-2023-23393	Elevation of Privilege	Important	No	No	2

			CVE-2023-23416	Remote Code Execution	Critical	No	No	1
5023755	高危	March 14, 2023— KB5023755 (Monthly Rollup) – Microsoft Support for Windows Server 2008 Datacenter ESU, Windows Server 2008 Standard ESU, Windows Server 2008 Enterprise ESU	CVE-2023-23422	Elevation of Privilege	Important	No	No	2
			CVE-2023-23415	Remote Code Execution	Critical	No	No	1
			CVE-2023-23423	Elevation of Privilege	Important	No	No	2
			CVE-2023-23420	Elevation of Privilege	Important	No	No	2
			CVE-2023-23405	Remote Code Execution	Important	No	No	2
			CVE-2023-23394	Information Disclosure	Important	No	No	2
			CVE-2023-21708	Remote Code Execution	Critical	No	No	2
			CVE-2023-24861	Elevation of Privilege	Important	No	No	1
			CVE-2023-23421	Elevation of Privilege	Important	No	No	2
			CVE-2023-24862	Denial of Service	Important	No	No	2
			CVE-2023-23409	Information Disclosure	Important	No	No	2
			CVE-2023-24910	Elevation of Privilege	Important	No	No	2
			CVE-2023-23410	Elevation of Privilege	Important	No	No	1
			CVE-2023-23385	Elevation of Privilege	Important	No	No	2
CVE-2023-24869	Remote Code Execution	Important	No	No	2			
CVE-2023-24908	Remote Code Execution	Important	No	No	2			
5023706	高危	March 14, 2023— KB5023706 (OS Build 22621.1413) –	CVE-2023-23394	Information Disclosure	Important	No	No	2
			CVE-2023-1018	Elevation of Privilege	Critical	No	No	2
			CVE-2023-23402	Remote Code Execution	Important	No	No	2

Microsoft Support for Windows 11 version 22H2, all editions	CVE-2023-24870	Information Disclosure	Important	No	No	2
	CVE-2023-24910	Elevation of Privilege	Important	No	No	2
	CVE-2023-23409	Information Disclosure	Important	No	No	2
	CVE-2023-23410	Elevation of Privilege	Important	No	No	1
	CVE-2023-23417	Elevation of Privilege	Important	No	No	2
	CVE-2023-24866	Information Disclosure	Important	No	No	2
	CVE-2023-23422	Elevation of Privilege	Important	No	No	2
	CVE-2023-24858	Information Disclosure	Important	No	No	2
	CVE-2023-23423	Elevation of Privilege	Important	No	No	2
	CVE-2023-23414	Remote Code Execution	Important	No	No	2
	CVE-2023-24868	Remote Code Execution	Important	No	No	2
	CVE-2023-23411	Denial of Service	Critical	No	No	2
	CVE-2023-24907	Remote Code Execution	Important	No	No	2
	CVE-2023-21708	Remote Code Execution	Critical	No	No	2
	CVE-2023-23421	Elevation of Privilege	Important	No	No	2
	CVE-2023-24862	Denial of Service	Important	No	No	2
	CVE-2023-23407	Remote Code Execution	Important	No	No	2
	CVE-2023-23392	Remote Code Execution	Critical	No	No	1
	CVE-2023-24869	Remote Code Execution	Important	No	No	2
	CVE-2023-23418	Elevation of Privilege	Important	No	No	2

			CVE-2023-23404	Remote Code Execution	Critical	No	No	2
			CVE-2023-24913	Remote Code Execution	Important	No	No	2
			CVE-2023-23413	Remote Code Execution	Important	No	No	2
			CVE-2023-23405	Remote Code Execution	Important	No	No	2
			CVE-2023-23420	Elevation of Privilege	Important	No	No	2
			CVE-2023-23401	Remote Code Execution	Important	No	No	2
			CVE-2023-24857	Information Disclosure	Important	No	No	2
			CVE-2023-24863	Information Disclosure	Important	No	No	2
			CVE-2023-24911	Information Disclosure	Important	No	No	2
			CVE-2023-1017	Elevation of Privilege	Critical	No	No	2
			CVE-2023-24861	Elevation of Privilege	Important	No	No	1
			CVE-2023-23403	Remote Code Execution	Important	No	No	2
			CVE-2023-23385	Elevation of Privilege	Important	No	No	2
			CVE-2023-24872	Remote Code Execution	Important	No	No	2
			CVE-2023-24876	Remote Code Execution	Important	No	No	2
			CVE-2023-24867	Remote Code Execution	Important	No	No	2
			CVE-2023-24906	Information Disclosure	Important	No	No	2
			CVE-2023-24908	Remote Code Execution	Important	No	No	2
			CVE-2023-23415	Remote Code Execution	Critical	No	No	1
			CVE-2023-23388	Elevation of Privilege	Important	No	No	2

			CVE-2023-24859	Denial of Service	Important	No	No	2
			CVE-2023-24856	Information Disclosure	Important	No	No	2
			CVE-2023-23406	Remote Code Execution	Important	No	No	2
			CVE-2023-24864	Elevation of Privilege	Important	No	No	2
			CVE-2023-23419	Elevation of Privilege	Important	No	No	2
			CVE-2023-24871	Remote Code Execution	Important	No	No	2
			CVE-2023-24865	Information Disclosure	Important	No	No	2
			CVE-2023-24909	Remote Code Execution	Important	No	No	2
			CVE-2023-24880	Security Feature Bypass	Moderate	Yes	Yes	0
			CVE-2023-23393	Elevation of Privilege	Important	No	No	2
			CVE-2023-23416	Remote Code Execution	Critical	No	No	1
			CVE-2023-23396	Denial of Service	Important	No	No	2
5023713	高危	March 14, 2023—KB5023713 (OS Build 10240.1980 5) - Microsoft Support for Windows 10	CVE-2023-23394	Information Disclosure	Important	No	No	2
			CVE-2023-1018	Elevation of Privilege	Critical	No	No	2
			CVE-2023-23402	Remote Code Execution	Important	No	No	2
			CVE-2023-24870	Information Disclosure	Important	No	No	2
			CVE-2023-24910	Elevation of Privilege	Important	No	No	2
			CVE-2023-23409	Information Disclosure	Important	No	No	2
			CVE-2023-23410	Elevation of Privilege	Important	No	No	1
			CVE-2023-24866	Information Disclosure	Important	No	No	2

		CVE-2023-23422	Elevation of Privilege	Important	No	No	2
		CVE-2023-24858	Information Disclosure	Important	No	No	2
		CVE-2023-23423	Elevation of Privilege	Important	No	No	2
		CVE-2023-23414	Remote Code Execution	Important	No	No	2
		CVE-2023-24868	Remote Code Execution	Important	No	No	2
		CVE-2023-23411	Denial of Service	Critical	No	No	2
		CVE-2023-24907	Remote Code Execution	Important	No	No	2
		CVE-2023-21708	Remote Code Execution	Critical	No	No	2
		CVE-2023-23421	Elevation of Privilege	Important	No	No	2
		CVE-2023-24862	Denial of Service	Important	No	No	2
		CVE-2023-23407	Remote Code Execution	Important	No	No	2
		CVE-2023-24869	Remote Code Execution	Important	No	No	2
		CVE-2023-23404	Remote Code Execution	Critical	No	No	2
		CVE-2023-24913	Remote Code Execution	Important	No	No	2
		CVE-2023-23413	Remote Code Execution	Important	No	No	2
		CVE-2023-23405	Remote Code Execution	Important	No	No	2
		CVE-2023-23420	Elevation of Privilege	Important	No	No	2
		CVE-2023-23401	Remote Code Execution	Important	No	No	2
		CVE-2023-24857	Information Disclosure	Important	No	No	2
		CVE-2023-24863	Information Disclosure	Important	No	No	2

			CVE-2023-24911	Information Disclosure	Important	No	No	2
			CVE-2023-1017	Elevation of Privilege	Critical	No	No	2
			CVE-2023-24861	Elevation of Privilege	Important	No	No	1
			CVE-2023-23403	Remote Code Execution	Important	No	No	2
			CVE-2023-23385	Elevation of Privilege	Important	No	No	2
			CVE-2023-24872	Remote Code Execution	Important	No	No	2
			CVE-2023-24876	Remote Code Execution	Important	No	No	2
			CVE-2023-24867	Remote Code Execution	Important	No	No	2
			CVE-2023-24906	Information Disclosure	Important	No	No	2
			CVE-2023-24908	Remote Code Execution	Important	No	No	2
			CVE-2023-23415	Remote Code Execution	Critical	No	No	1
			CVE-2023-24859	Denial of Service	Important	No	No	2
			CVE-2023-24856	Information Disclosure	Important	No	No	2
			CVE-2023-23406	Remote Code Execution	Important	No	No	2
			CVE-2023-24864	Elevation of Privilege	Important	No	No	2
			CVE-2023-23412	Elevation of Privilege	Important	No	No	2
			CVE-2023-24865	Information Disclosure	Important	No	No	2
			CVE-2023-24909	Remote Code Execution	Important	No	No	2
			CVE-2023-23416	Remote Code Execution	Critical	No	No	1
5023759	高危	March 14, 2023—	CVE-2023-23394	Information Disclosure	Important	No	No	2

		KB5023759 (Security-only update) - Microsoft Support for Windows Server 2008 R2 Enterprise ESU, Windows Server 2008 R2 Standard ESU, Windows Server 2008 R2 Datacenter ESU, Windows Embedded Standard 7 ESU, Windows Embedded POSReady 7 ESU	CVE-2023-23402	Remote Code Execution	Important	No	No	2
			CVE-2023-23409	Information Disclosure	Important	No	No	2
			CVE-2023-24910	Elevation of Privilege	Important	No	No	2
			CVE-2023-23410	Elevation of Privilege	Important	No	No	1
			CVE-2023-23422	Elevation of Privilege	Important	No	No	2
			CVE-2023-23423	Elevation of Privilege	Important	No	No	2
			CVE-2023-23414	Remote Code Execution	Important	No	No	2
			CVE-2023-21708	Remote Code Execution	Critical	No	No	2
			CVE-2023-23421	Elevation of Privilege	Important	No	No	2
			CVE-2023-24862	Denial of Service	Important	No	No	2
			CVE-2023-23407	Remote Code Execution	Important	No	No	2
			CVE-2023-24869	Remote Code Execution	Important	No	No	2
			CVE-2023-23405	Remote Code Execution	Important	No	No	2
			CVE-2023-23420	Elevation of Privilege	Important	No	No	2
			CVE-2023-23401	Remote Code Execution	Important	No	No	2
			CVE-2023-24861	Elevation of Privilege	Important	No	No	1
			CVE-2023-23385	Elevation of Privilege	Important	No	No	2
CVE-2023-24908	Remote Code Execution	Important	No	No	2			
CVE-2023-23415	Remote Code Execution	Critical	No	No	1			
5023769	高危	March 14, 2023—	CVE-2023-23394	Information Disclosure	Important	No	No	2

		KB5023769 (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-2023-23402	Remote Code Execution	Important	No	No	2
			CVE-2023-23409	Information Disclosure	Important	No	No	2
			CVE-2023-24910	Elevation of Privilege	Important	No	No	2
			CVE-2023-23410	Elevation of Privilege	Important	No	No	1
			CVE-2023-23422	Elevation of Privilege	Important	No	No	2
			CVE-2023-23423	Elevation of Privilege	Important	No	No	2
			CVE-2023-23414	Remote Code Execution	Important	No	No	2
			CVE-2023-21708	Remote Code Execution	Critical	No	No	2
			CVE-2023-23421	Elevation of Privilege	Important	No	No	2
			CVE-2023-24862	Denial of Service	Important	No	No	2
			CVE-2023-23407	Remote Code Execution	Important	No	No	2
			CVE-2023-24869	Remote Code Execution	Important	No	No	2
			CVE-2023-23405	Remote Code Execution	Important	No	No	2
			CVE-2023-23420	Elevation of Privilege	Important	No	No	2
			CVE-2023-23401	Remote Code Execution	Important	No	No	2
			CVE-2023-24861	Elevation of Privilege	Important	No	No	1
CVE-2023-23385	Elevation of Privilege	Important	No	No	2			
CVE-2023-24908	Remote Code Execution	Important	No	No	2			
CVE-2023-23415	Remote Code Execution	Critical	No	No	1			
5023765	高危	March 14, 2023—	CVE-2023-23394	Information Disclosure	Important	No	No	2

KB5023765 (Monthly Rollup) – Microsoft Support for Windows Server 2012 R2, Windows Embedded 8.1 Industry Enterprise, Windows Embedded 8.1 Industry Pro	CVE-2023-23402	Remote Code Execution	Important	No	No	2
	CVE-2023-24870	Information Disclosure	Important	No	No	2
	CVE-2023-24910	Elevation of Privilege	Important	No	No	2
	CVE-2023-23409	Information Disclosure	Important	No	No	2
	CVE-2023-23410	Elevation of Privilege	Important	No	No	1
	CVE-2023-24866	Information Disclosure	Important	No	No	2
	CVE-2023-23422	Elevation of Privilege	Important	No	No	2
	CVE-2023-24858	Information Disclosure	Important	No	No	2
	CVE-2023-23423	Elevation of Privilege	Important	No	No	2
	CVE-2023-23414	Remote Code Execution	Important	No	No	2
	CVE-2023-24868	Remote Code Execution	Important	No	No	2
	CVE-2023-24907	Remote Code Execution	Important	No	No	2
	CVE-2023-21708	Remote Code Execution	Critical	No	No	2
	CVE-2023-23421	Elevation of Privilege	Important	No	No	2
	CVE-2023-24862	Denial of Service	Important	No	No	2
	CVE-2023-23407	Remote Code Execution	Important	No	No	2
	CVE-2023-24869	Remote Code Execution	Important	No	No	2
	CVE-2023-23404	Remote Code Execution	Critical	No	No	2
	CVE-2023-24913	Remote Code Execution	Important	No	No	2
CVE-2023-23413	Remote Code Execution	Important	No	No	2	

			CVE-2023-23405	Remote Code Execution	Important	No	No	2
			CVE-2023-23420	Elevation of Privilege	Important	No	No	2
			CVE-2023-23401	Remote Code Execution	Important	No	No	2
			CVE-2023-24857	Information Disclosure	Important	No	No	2
			CVE-2023-23400	Remote Code Execution	Important	No	No	2
			CVE-2023-24863	Information Disclosure	Important	No	No	2
			CVE-2023-24911	Information Disclosure	Important	No	No	2
			CVE-2023-24861	Elevation of Privilege	Important	No	No	1
			CVE-2023-23403	Remote Code Execution	Important	No	No	2
			CVE-2023-23385	Elevation of Privilege	Important	No	No	2
			CVE-2023-24872	Remote Code Execution	Important	No	No	2
			CVE-2023-24876	Remote Code Execution	Important	No	No	2
			CVE-2023-24867	Remote Code Execution	Important	No	No	2
			CVE-2023-24906	Information Disclosure	Important	No	No	2
			CVE-2023-24908	Remote Code Execution	Important	No	No	2
			CVE-2023-23415	Remote Code Execution	Critical	No	No	1
			CVE-2023-24859	Denial of Service	Important	No	No	2
			CVE-2023-24856	Information Disclosure	Important	No	No	2
			CVE-2023-23406	Remote Code Execution	Important	No	No	2
			CVE-2023-24864	Elevation of Privilege	Important	No	No	2

			CVE-2023-23412	Elevation of Privilege	Important	No	No	2
			CVE-2023-24865	Information Disclosure	Important	No	No	2
			CVE-2023-24909	Remote Code Execution	Important	No	No	2
			CVE-2023-23416	Remote Code Execution	Critical	No	No	1
5023752	高危	March 14, 2023—KB5023752 (Security-only update) – Microsoft Support for Windows Server 2012, Windows Embedded 8 Standard	CVE-2023-23394	Information Disclosure	Important	No	No	2
			CVE-2023-23402	Remote Code Execution	Important	No	No	2
			CVE-2023-24870	Information Disclosure	Important	No	No	2
			CVE-2023-24910	Elevation of Privilege	Important	No	No	2
			CVE-2023-23409	Information Disclosure	Important	No	No	2
			CVE-2023-23410	Elevation of Privilege	Important	No	No	1
			CVE-2023-24866	Information Disclosure	Important	No	No	2
			CVE-2023-23422	Elevation of Privilege	Important	No	No	2
			CVE-2023-24858	Information Disclosure	Important	No	No	2
			CVE-2023-23423	Elevation of Privilege	Important	No	No	2
			CVE-2023-23414	Remote Code Execution	Important	No	No	2
			CVE-2023-24868	Remote Code Execution	Important	No	No	2
			CVE-2023-24907	Remote Code Execution	Important	No	No	2
			CVE-2023-21708	Remote Code Execution	Critical	No	No	2
			CVE-2023-23421	Elevation of Privilege	Important	No	No	2
			CVE-2023-24862	Denial of Service	Important	No	No	2

			CVE-2023-23407	Remote Code Execution	Important	No	No	2
			CVE-2023-24869	Remote Code Execution	Important	No	No	2
			CVE-2023-23404	Remote Code Execution	Critical	No	No	2
			CVE-2023-24913	Remote Code Execution	Important	No	No	2
			CVE-2023-23413	Remote Code Execution	Important	No	No	2
			CVE-2023-23405	Remote Code Execution	Important	No	No	2
			CVE-2023-23420	Elevation of Privilege	Important	No	No	2
			CVE-2023-23401	Remote Code Execution	Important	No	No	2
			CVE-2023-24857	Information Disclosure	Important	No	No	2
			CVE-2023-24863	Information Disclosure	Important	No	No	2
			CVE-2023-24911	Information Disclosure	Important	No	No	2
			CVE-2023-24861	Elevation of Privilege	Important	No	No	1
			CVE-2023-23403	Remote Code Execution	Important	No	No	2
			CVE-2023-23385	Elevation of Privilege	Important	No	No	2
			CVE-2023-24876	Remote Code Execution	Important	No	No	2
			CVE-2023-24867	Remote Code Execution	Important	No	No	2
			CVE-2023-24906	Information Disclosure	Important	No	No	2
			CVE-2023-24908	Remote Code Execution	Important	No	No	2
			CVE-2023-23415	Remote Code Execution	Critical	No	No	1
			CVE-2023-24859	Denial of Service	Important	No	No	2

			CVE-2023-24856	Information Disclosure	Important	No	No	2
			CVE-2023-23406	Remote Code Execution	Important	No	No	2
			CVE-2023-24864	Elevation of Privilege	Important	No	No	2
			CVE-2023-23412	Elevation of Privilege	Important	No	No	2
			CVE-2023-24865	Information Disclosure	Important	No	No	2
			CVE-2023-24909	Remote Code Execution	Important	No	No	2
			CVE-2023-23416	Remote Code Execution	Critical	No	No	1
5023754	高危	March 14, 2023—KB5023754 (Security-only update) - Microsoft Support for Windows Server 2008 Datacenter ESU, Windows Server 2008 Standard ESU, Windows Server 2008 Enterprise ESU	CVE-2023-23422	Elevation of Privilege	Important	No	No	2
			CVE-2023-23415	Remote Code Execution	Critical	No	No	1
			CVE-2023-23423	Elevation of Privilege	Important	No	No	2
			CVE-2023-23420	Elevation of Privilege	Important	No	No	2
			CVE-2023-23405	Remote Code Execution	Important	No	No	2
			CVE-2023-23394	Information Disclosure	Important	No	No	2
			CVE-2023-21708	Remote Code Execution	Critical	No	No	2
			CVE-2023-24861	Elevation of Privilege	Important	No	No	1
			CVE-2023-23421	Elevation of Privilege	Important	No	No	2
			CVE-2023-24862	Denial of Service	Important	No	No	2
			CVE-2023-23409	Information Disclosure	Important	No	No	2
			CVE-2023-24910	Elevation of Privilege	Important	No	No	2
			CVE-2023-23410	Elevation of Privilege	Important	No	No	1

			CVE-2023-23385	Elevation of Privilege	Important	No	No	2
			CVE-2023-24869	Remote Code Execution	Important	No	No	2
			CVE-2023-24908	Remote Code Execution	Important	No	No	2

本月微软发布的软件安全更新补丁共 7 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
5002348	高危	Description of the security update for Excel 2013: March 14, 2023 (KB5002348) - Microsoft Support	CVE-2023-23399	Remote Code Execution	Important	No	No	2
			CVE-2023-23398	Spoofing	Important	No	No	1
5002254	高危	Description of the security update for Outlook 2016: March 14, 2023 (KB5002254) -	CVE-2023-23397	Elevation of Privilege	Critical	No	Yes	0

		Microsoft Support						
5002362	高危	Description of the security update for Office Web Apps Server 2013: March 14, 2023 (KB5002362) - Microsoft Support	CVE-2023-23399	Remote Code Execution	Important	No	No	2
5002197	高危	Description of the security update for Office 2016: March 14, 2023 (KB5002197) - Microsoft Support	CVE-2023-23399	Remote Code Execution	Important	No	No	2
5002198	高危	Description of the security update for Office 2013: March 14, 2023 (KB5002198) -	CVE-2023-23399	Remote Code Execution	Important	No	No	2

		Microsoft Support						
5002351	高危	Description of the security update for Excel 2016: March 14, 2023 (KB5002351) - Microsoft Support	CVE-2023-23399	Remote Code Execution	Important	No	No	2
			CVE-2023-23398	Spoofing	Important	No	No	1
5002265	高危	Description of the security update for Outlook 2013: March 14, 2023 (KB5002265) - Microsoft Support	CVE-2023-23397	Elevation of Privilege	Critical	No	Yes	0

本月发布内容中一般性更新补丁:

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>