

奇安信集团 2023 年 6 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 6 月 14 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.....	37

文档信息

文档名称	奇安信集团 2023 年 6 月补丁库更新通告		
文档编号	Qi An Xin Group-MSPatch-2023-0601		
发布日期	2023-06-14	密级	公开
关键字	Microsoft、漏洞、补丁		
发布团队	奇安信集团漏洞补丁运营团队		

第1章 安全通告

尊敬的客户：

奇安信集团最新补丁库(V6 版本:2023.06.14.1,V10 版本:2023.06.14.1000)已发布,本次更新推送了 37 个微软安全补丁,修复了 50 个安全漏洞,其中 5 个微软官方评级为“严重(Critical)”,45 个评级为“重要(Important)”,这些漏洞影响 Windows、.NET Framework、Office 等产品。

第2章 重点关注补丁

本月有 13 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
5027533	CVE-2023-24897	Remote Code Execution	Critical	No	No	Exploitation Less Likely
5027119						
5027537						
5027539						
5027536						
5027531						
5027542						
5027540						
5027544						
5027538						
5027219						
5027543						
5027534						
5027230						
5027541						
5027123						
5027532						
5026261	CVE-2023-28310	Remote Code Execution	Important	No	No	Exploitation More Likely
5025903						
5026261	CVE-2023-32031	Remote Code Execution	Important	No	No	Exploitation More Likely
5025903						
5027225	CVE-2023-32015	Remote Code Execution	Critical	No	No	Exploitation Less Likely
5027275						
5027222						
5027256						
5027231						
5027282						
5027219						

5027277						
5027279						
5027215						
5027283						
5027230						
5027271						
5027281						
5027223						
5027225	CVE-2023-29361	Elevation of Privilege	Important	No	No	Exploitation More Likely
5027231						
5027215						
5027223						
5027225	CVE-2023-32014	Remote Code Execution	Critical	No	No	Exploitation Less Likely
5027275						
5027222						
5027256						
5027231						
5027282						
5027219						
5027277						
5027279						
5027215						
5027283						
5027230						
5027271						
5027281						
5027223						
5027225	CVE-2023-29363	Remote Code Execution	Critical	No	No	Exploitation Less Likely
5027275						
5027222						
5027256						
5027231						
5027282						
5027219						
5027277						
5027279						
5027215						
5027283						
5027230						
5027271						
5027281						

5027223						
5027225	CVE-2023-29358	Elevation of Privilege	Important	No	No	Exploitation More Likely
5027275						
5027222						
5027256						
5027231						
5027282						
5027219						
5027277						
5027279						
5027215						
5027283						
5027230						
5027271						
5027281						
5027223						
5027225	CVE-2023-29360	Elevation of Privilege	Important	No	No	Exploitation More Likely
5027222						
5027231						
5027219						
5027215						
5027223						
5027225	CVE-2023-29359	Elevation of Privilege	Important	No	No	Exploitation More Likely
5027275						
5027222						
5027256						
5027231						
5027282						
5027219						
5027277						
5027279						
5027215						
5027283						
5027230						
5027271						
5027281						
5027223						
5027225	CVE-2023-29371	Elevation of Privilege	Important	No	No	Exploitation More Likely
5027275						
5027222						
5027256						

5027231						
5027282						
5027219						
5027277						
5027279						
5027215						
5027283						
5027230						
5027271						
5027281						
5027223						
5027225	CVE-2023-32013	Denial of Service	Critical	No	No	Exploitation Less Likely
5027222						
5027231						
5027215						
5027223						

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 16 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
5026261	高危	Description of the security update for Microsoft Exchange Server 2019: June 13, 2023 (KB5026261) - Microsoft Support	CVE-2023-28310	Remote Code Execution	Important	No	No	1
			CVE-2023-32031	Remote Code Execution	Important	No	No	1
5027225	高危	June 13, 2023—KB5027225 (OS Build 20348.1787) - Microsoft Support for Windows Server 2022	CVE-2023-32017	Remote Code Execution	Important	No	No	2
			CVE-2023-32015	Remote Code Execution	Critical	No	No	2
			CVE-2023-29366	Remote Code Execution	Important	No	No	2
			CVE-2023-29364	Elevation of Privilege	Important	No	No	2
			CVE-2023-32020	Spoofing	Important	No	No	2
			CVE-2023-29361	Elevation of Privilege	Important	No	No	1
			CVE-2023-32014	Remote Code Execution	Critical	No	No	2
			CVE-2023-29370	Remote Code Execution	Important	No	No	2
			CVE-2023-29363	Remote Code Execution	Critical	No	No	2

			CVE-2023-29369	Denial of Service	Important	No	No	2
			CVE-2023-29367	Remote Code Execution	Important	No	No	2
			CVE-2023-29358	Elevation of Privilege	Important	No	No	1
			CVE-2023-29372	Remote Code Execution	Important	No	No	2
			CVE-2023-29351	Elevation of Privilege	Important	No	No	2
			CVE-2023-29373	Remote Code Execution	Important	No	No	2
			CVE-2023-29360	Elevation of Privilege	Important	No	No	1
			CVE-2023-29355	Information Disclosure	Important	No	No	2
			CVE-2023-29346	Elevation of Privilege	Important	No	No	2
			CVE-2023-32016	Information Disclosure	Important	No	No	2
			CVE-2023-32019	Information Disclosure	Important	No	No	2
			CVE-2023-32021	Security Feature Bypass	Important	No	No	2
			CVE-2023-32008	Remote Code Execution	Important	No	No	2
			CVE-2023-29365	Remote Code Execution	Important	No	No	2
			CVE-2023-29359	Elevation of Privilege	Important	No	No	1
			CVE-2023-24937	Denial of Service	Important	No	No	2
			CVE-2023-24938	Denial of Service	Important	No	No	2
			CVE-2023-29352	Security Feature Bypass	Important	No	No	2
			CVE-2023-29371	Elevation of Privilege	Important	No	No	1

			CVE-2023-32013	Denial of Service	Critical	No	No	2
			CVE-2023-29362	Remote Code Execution	Important	No	No	2
			CVE-2023-32022	Security Feature Bypass	Important	No	No	2
			CVE-2023-32011	Denial of Service	Important	No	No	2
			CVE-2023-32009	Elevation of Privilege	Important	No	No	2
			CVE-2023-29368	Elevation of Privilege	Important	No	No	2
5027275	高危	June 13, 2023—KB5027275 (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-2023-32017	Remote Code Execution	Important	No	No	2
			CVE-2023-32015	Remote Code Execution	Critical	No	No	2
			CVE-2023-29363	Remote Code Execution	Critical	No	No	2
			CVE-2023-29365	Remote Code Execution	Important	No	No	2
			CVE-2023-29358	Elevation of Privilege	Important	No	No	1
			CVE-2023-29372	Remote Code Execution	Important	No	No	2
			CVE-2023-29359	Elevation of Privilege	Important	No	No	1
			CVE-2023-29351	Elevation of Privilege	Important	No	No	2
			CVE-2023-29373	Remote Code Execution	Important	No	No	2
			CVE-2023-32011	Denial of Service	Important	No	No	2
			CVE-2023-29364	Elevation of Privilege	Important	No	No	2
			CVE-2023-32020	Spoofing	Important	No	No	2
			CVE-2023-29368	Elevation of Privilege	Important	No	No	2
			CVE-2023-29371	Elevation of Privilege	Important	No	No	1

			CVE-2023-29346	Elevation of Privilege	Important	No	No	2
			CVE-2023-32016	Information Disclosure	Important	No	No	2
			CVE-2023-32014	Remote Code Execution	Critical	No	No	2
			CVE-2023-29362	Remote Code Execution	Important	No	No	2
5027222	高危	June 13, 2023— KB5027222 (OS Build 17763.4499) - Microsoft Support for Win 10 Ent LTSC v2019, Win 10 IoT Ent LTSC v2019, Windows 10 IoT Core 2019 LTSC, Windows Server 2019	CVE-2023-32017	Remote Code Execution	Important	No	No	2
			CVE-2023-32015	Remote Code Execution	Critical	No	No	2
			CVE-2023-29364	Elevation of Privilege	Important	No	No	2
			CVE-2023-32020	Spoofing	Important	No	No	2
			CVE-2023-32014	Remote Code Execution	Critical	No	No	2
			CVE-2023-29370	Remote Code Execution	Important	No	No	2
			CVE-2023-29363	Remote Code Execution	Critical	No	No	2
			CVE-2023-29369	Denial of Service	Important	No	No	2
			CVE-2023-29367	Remote Code Execution	Important	No	No	2
			CVE-2023-29358	Elevation of Privilege	Important	No	No	1
			CVE-2023-29372	Remote Code Execution	Important	No	No	2
			CVE-2023-29351	Elevation of Privilege	Important	No	No	2
			CVE-2023-29373	Remote Code Execution	Important	No	No	2
			CVE-2023-29360	Elevation of Privilege	Important	No	No	1
			CVE-2023-29355	Information Disclosure	Important	No	No	2
CVE-2023-29346	Elevation of Privilege	Important	No	No	2			
CVE-2023-32016	Information Disclosure	Important	No	No	2			

			CVE-2023-32019	Information Disclosure	Important	No	No	2
			CVE-2023-32021	Security Feature Bypass	Important	No	No	2
			CVE-2023-32008	Remote Code Execution	Important	No	No	2
			CVE-2023-29365	Remote Code Execution	Important	No	No	2
			CVE-2023-29359	Elevation of Privilege	Important	No	No	1
			CVE-2023-24937	Denial of Service	Important	No	No	2
			CVE-2023-24938	Denial of Service	Important	No	No	2
			CVE-2023-29352	Security Feature Bypass	Important	No	No	2
			CVE-2023-29371	Elevation of Privilege	Important	No	No	1
			CVE-2023-32013	Denial of Service	Critical	No	No	2
			CVE-2023-29362	Remote Code Execution	Important	No	No	2
			CVE-2023-32022	Security Feature Bypass	Important	No	No	2
			CVE-2023-32011	Denial of Service	Important	No	No	2
			CVE-2023-32009	Elevation of Privilege	Important	No	No	2
			CVE-2023-29368	Elevation of Privilege	Important	No	No	2
5027256	高危	June 13, 2023—KB5027256 (Security-only update) - Microsoft Support for Windows	CVE-2023-32017	Remote Code Execution	Important	No	No	2
			CVE-2023-32015	Remote Code Execution	Critical	No	No	2
			CVE-2023-29363	Remote Code Execution	Critical	No	No	2
			CVE-2023-29365	Remote Code Execution	Important	No	No	2

		Server 2008 R2	CVE-2023-29358	Elevation of Privilege	Important	No	No	1
		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-2023-29372	Remote Code Execution	Important	No	No	2
			CVE-2023-29359	Elevation of Privilege	Important	No	No	1
			CVE-2023-29351	Elevation of Privilege	Important	No	No	2
			CVE-2023-29373	Remote Code Execution	Important	No	No	2
			CVE-2023-32011	Denial of Service	Important	No	No	2
			CVE-2023-29364	Elevation of Privilege	Important	No	No	2
			CVE-2023-32020	Spoofing	Important	No	No	2
			CVE-2023-29368	Elevation of Privilege	Important	No	No	2
			CVE-2023-29371	Elevation of Privilege	Important	No	No	1
			CVE-2023-29346	Elevation of Privilege	Important	No	No	2
			CVE-2023-32016	Information Disclosure	Important	No	No	2
			CVE-2023-32014	Remote Code Execution	Critical	No	No	2
			CVE-2023-29362	Remote Code Execution	Important	No	No	2
5027231	高危	June 13, 2023—KB5027231 (OS Build 22621.1848) - Microsoft Support for Windows 11 version 22H2, all editions	CVE-2023-32015	Remote Code Execution	Critical	No	No	2
			CVE-2023-32017	Remote Code Execution	Important	No	No	2
			CVE-2023-29366	Remote Code Execution	Important	No	No	2
			CVE-2023-29364	Elevation of Privilege	Important	No	No	2
			CVE-2023-29361	Elevation of Privilege	Important	No	No	1
			CVE-2023-32014	Remote Code Execution	Critical	No	No	2
			CVE-2023-29370	Remote Code Execution	Important	No	No	2

			CVE-2023-29363	Remote Code Execution	Critical	No	No	2
			CVE-2023-29358	Elevation of Privilege	Important	No	No	1
			CVE-2023-29372	Remote Code Execution	Important	No	No	2
			CVE-2023-29351	Elevation of Privilege	Important	No	No	2
			CVE-2023-32018	Remote Code Execution	Important	No	No	2
			CVE-2023-29373	Remote Code Execution	Important	No	No	2
			CVE-2023-29360	Elevation of Privilege	Important	No	No	1
			CVE-2023-29346	Elevation of Privilege	Important	No	No	2
			CVE-2023-32016	Information Disclosure	Important	No	No	2
			CVE-2023-32019	Information Disclosure	Important	No	No	2
			CVE-2023-32008	Remote Code Execution	Important	No	No	2
			CVE-2023-29365	Remote Code Execution	Important	No	No	2
			CVE-2023-32012	Elevation of Privilege	Important	No	No	2
			CVE-2023-29359	Elevation of Privilege	Important	No	No	1
			CVE-2023-24937	Denial of Service	Important	No	No	2
			CVE-2023-24938	Denial of Service	Important	No	No	2
			CVE-2023-32010	Elevation of Privilege	Important	No	No	2
			CVE-2023-29352	Security Feature Bypass	Important	No	No	2
			CVE-2023-29371	Elevation of Privilege	Important	No	No	1
			CVE-2023-32013	Denial of Service	Critical	No	No	2

			CVE-2023-29362	Remote Code Execution	Important	No	No	2
			CVE-2023-32011	Denial of Service	Important	No	No	2
			CVE-2023-32009	Elevation of Privilege	Important	No	No	2
			CVE-2023-29368	Elevation of Privilege	Important	No	No	2
5027282	高危	June 13, 2023—KB5027282 (Security-only update) - Microsoft Support for Windows Server 2012 R2, Windows Embedded 8.1 Industry Enterprise, Windows Embedded 8.1 Industry Pro	CVE-2023-32017	Remote Code Execution	Important	No	No	2
			CVE-2023-32015	Remote Code Execution	Critical	No	No	2
			CVE-2023-29364	Elevation of Privilege	Important	No	No	2
			CVE-2023-32020	Spoofing	Important	No	No	2
			CVE-2023-32014	Remote Code Execution	Critical	No	No	2
			CVE-2023-29363	Remote Code Execution	Critical	No	No	2
			CVE-2023-29369	Denial of Service	Important	No	No	2
			CVE-2023-29367	Remote Code Execution	Important	No	No	2
			CVE-2023-29358	Elevation of Privilege	Important	No	No	1
			CVE-2023-29372	Remote Code Execution	Important	No	No	2
			CVE-2023-29351	Elevation of Privilege	Important	No	No	2
			CVE-2023-29373	Remote Code Execution	Important	No	No	2
			CVE-2023-29355	Information Disclosure	Important	No	No	2
			CVE-2023-29346	Elevation of Privilege	Important	No	No	2
			CVE-2023-32016	Information Disclosure	Important	No	No	2
			CVE-2023-32021	Security Feature Bypass	Important	No	No	2

			CVE-2023-29365	Remote Code Execution	Important	No	No	2
			CVE-2023-29359	Elevation of Privilege	Important	No	No	1
			CVE-2023-29371	Elevation of Privilege	Important	No	No	1
			CVE-2023-29362	Remote Code Execution	Important	No	No	2
			CVE-2023-32022	Security Feature Bypass	Important	No	No	2
			CVE-2023-32011	Denial of Service	Important	No	No	2
			CVE-2023-29368	Elevation of Privilege	Important	No	No	2
5027219	高危	June 13, 2023—KB5027219 (OS Build 14393.5989) – Microsoft Support for Windows 10, version 1607, all editions, Windows Server 2016, all editions	CVE-2023-32017	Remote Code Execution	Important	No	No	2
			CVE-2023-32015	Remote Code Execution	Critical	No	No	2
			CVE-2023-32030	Denial of Service	Important	No	No	2
			CVE-2023-29326	Remote Code Execution	Important	No	No	2
			CVE-2023-29364	Elevation of Privilege	Important	No	No	2
			CVE-2023-32020	Spoofing	Important	No	No	2
			CVE-2023-24897	Remote Code Execution	Critical	No	No	2
			CVE-2023-32014	Remote Code Execution	Critical	No	No	2
			CVE-2023-29370	Remote Code Execution	Important	No	No	2
			CVE-2023-29363	Remote Code Execution	Critical	No	No	2
			CVE-2023-29369	Denial of Service	Important	No	No	2
			CVE-2023-29367	Remote Code Execution	Important	No	No	2
			CVE-2023-29358	Elevation of Privilege	Important	No	No	1

			CVE-2023-29372	Remote Code Execution	Important	No	No	2
			CVE-2023-29351	Elevation of Privilege	Important	No	No	2
			CVE-2023-29373	Remote Code Execution	Important	No	No	2
			CVE-2023-29360	Elevation of Privilege	Important	No	No	1
			CVE-2023-29355	Information Disclosure	Important	No	No	2
			CVE-2023-29346	Elevation of Privilege	Important	No	No	2
			CVE-2023-32016	Information Disclosure	Important	No	No	2
			CVE-2023-32019	Information Disclosure	Important	No	No	2
			CVE-2023-32021	Security Feature Bypass	Important	No	No	2
			CVE-2023-32008	Remote Code Execution	Important	No	No	2
			CVE-2023-29365	Remote Code Execution	Important	No	No	2
			CVE-2023-24895	Remote Code Execution	Important	No	No	2
			CVE-2023-29359	Elevation of Privilege	Important	No	No	1
			CVE-2023-29371	Elevation of Privilege	Important	No	No	1
			CVE-2023-29362	Remote Code Execution	Important	No	No	2
			CVE-2023-24936	Elevation of Privilege	Moderate	No	No	2
			CVE-2023-32022	Security Feature Bypass	Important	No	No	2
			CVE-2023-32011	Denial of Service	Important	No	No	2
			CVE-2023-32009	Elevation of Privilege	Important	No	No	2

			CVE-2023-29331	Denial of Service	Important	No	No	2
			CVE-2023-29368	Elevation of Privilege	Important	No	No	2
5027277	高危	June 13, 2023—KB5027277 (Security-only update) - Microsoft Support for Windows Server 2008 Datacenter ESU, Windows Server 2008 Standard ESU, Windows Server 2008 Enterprise ESU	CVE-2023-32017	Remote Code Execution	Important	No	No	2
			CVE-2023-32015	Remote Code Execution	Critical	No	No	2
			CVE-2023-29363	Remote Code Execution	Critical	No	No	2
			CVE-2023-29358	Elevation of Privilege	Important	No	No	1
			CVE-2023-29372	Remote Code Execution	Important	No	No	2
			CVE-2023-29359	Elevation of Privilege	Important	No	No	1
			CVE-2023-29351	Elevation of Privilege	Important	No	No	2
			CVE-2023-29373	Remote Code Execution	Important	No	No	2
			CVE-2023-32011	Denial of Service	Important	No	No	2
			CVE-2023-32020	Spoofing	Important	No	No	2
			CVE-2023-29368	Elevation of Privilege	Important	No	No	2
			CVE-2023-29371	Elevation of Privilege	Important	No	No	1
			CVE-2023-29346	Elevation of Privilege	Important	No	No	2
			CVE-2023-32016	Information Disclosure	Important	No	No	2
CVE-2023-32014	Remote Code Execution	Critical	No	No	2			
5027279	高危	June 13, 2023—KB5027279 (Monthly Rollup) - Microsoft Support for Windows	CVE-2023-32017	Remote Code Execution	Important	No	No	2
			CVE-2023-32015	Remote Code Execution	Critical	No	No	2
			CVE-2023-29363	Remote Code Execution	Critical	No	No	2
			CVE-2023-29358	Elevation of Privilege	Important	No	No	1

		Server 2008 Datacenter ESU, Windows Server 2008 Standard ESU, Windows Server 2008 Enterprise ESU	CVE-2023-29372	Remote Code Execution	Important	No	No	2
			CVE-2023-29359	Elevation of Privilege	Important	No	No	1
			CVE-2023-29351	Elevation of Privilege	Important	No	No	2
			CVE-2023-29373	Remote Code Execution	Important	No	No	2
			CVE-2023-32011	Denial of Service	Important	No	No	2
			CVE-2023-32020	Spoofing	Important	No	No	2
			CVE-2023-29368	Elevation of Privilege	Important	No	No	2
			CVE-2023-29371	Elevation of Privilege	Important	No	No	1
			CVE-2023-29346	Elevation of Privilege	Important	No	No	2
			CVE-2023-32016	Information Disclosure	Important	No	No	2
			CVE-2023-32014	Remote Code Execution	Critical	No	No	2
5027215	高危	June 13, 2023—KB5027215 (OS Builds 19044.3086 and 19045.3086) – Microsoft Support for Windows 10, version 21H2, all editions, Windows 10, version 22H2, all editions	CVE-2023-32015	Remote Code Execution	Critical	No	No	2
			CVE-2023-32017	Remote Code Execution	Important	No	No	2
			CVE-2023-29366	Remote Code Execution	Important	No	No	2
			CVE-2023-29364	Elevation of Privilege	Important	No	No	2
			CVE-2023-29361	Elevation of Privilege	Important	No	No	1
			CVE-2023-32014	Remote Code Execution	Critical	No	No	2
			CVE-2023-29370	Remote Code Execution	Important	No	No	2
			CVE-2023-29363	Remote Code Execution	Critical	No	No	2
			CVE-2023-29358	Elevation of Privilege	Important	No	No	1
			CVE-2023-29372	Remote Code Execution	Important	No	No	2

			CVE-2023-29351	Elevation of Privilege	Important	No	No	2
			CVE-2023-29373	Remote Code Execution	Important	No	No	2
			CVE-2023-29360	Elevation of Privilege	Important	No	No	1
			CVE-2023-29346	Elevation of Privilege	Important	No	No	2
			CVE-2023-32016	Information Disclosure	Important	No	No	2
			CVE-2023-32019	Information Disclosure	Important	No	No	2
			CVE-2023-32008	Remote Code Execution	Important	No	No	2
			CVE-2023-29365	Remote Code Execution	Important	No	No	2
			CVE-2023-32012	Elevation of Privilege	Important	No	No	2
			CVE-2023-29359	Elevation of Privilege	Important	No	No	1
			CVE-2023-24937	Denial of Service	Important	No	No	2
			CVE-2023-24938	Denial of Service	Important	No	No	2
			CVE-2023-29352	Security Feature Bypass	Important	No	No	2
			CVE-2023-29371	Elevation of Privilege	Important	No	No	1
			CVE-2023-32013	Denial of Service	Critical	No	No	2
			CVE-2023-29362	Remote Code Execution	Important	No	No	2
			CVE-2023-32011	Denial of Service	Important	No	No	2
			CVE-2023-32009	Elevation of Privilege	Important	No	No	2
			CVE-2023-29368	Elevation of Privilege	Important	No	No	2
5027283	高危	June 13, 2023—	CVE-2023-32017	Remote Code Execution	Important	No	No	2

		KB5027283 (Monthly Rollup) - Microsoft Support for Windows Server 2012, Windows Embedded 8 Standard	CVE-2023-32015	Remote Code Execution	Critical	No	No	2
			CVE-2023-29364	Elevation of Privilege	Important	No	No	2
			CVE-2023-32020	Spoofing	Important	No	No	2
			CVE-2023-32014	Remote Code Execution	Critical	No	No	2
			CVE-2023-29363	Remote Code Execution	Critical	No	No	2
			CVE-2023-29369	Denial of Service	Important	No	No	2
			CVE-2023-29358	Elevation of Privilege	Important	No	No	1
			CVE-2023-29372	Remote Code Execution	Important	No	No	2
			CVE-2023-29351	Elevation of Privilege	Important	No	No	2
			CVE-2023-29373	Remote Code Execution	Important	No	No	2
			CVE-2023-29355	Information Disclosure	Important	No	No	2
			CVE-2023-29346	Elevation of Privilege	Important	No	No	2
			CVE-2023-32016	Information Disclosure	Important	No	No	2
			CVE-2023-29365	Remote Code Execution	Important	No	No	2
			CVE-2023-29359	Elevation of Privilege	Important	No	No	1
			CVE-2023-29371	Elevation of Privilege	Important	No	No	1
			CVE-2023-29362	Remote Code Execution	Important	No	No	2
			CVE-2023-32011	Denial of Service	Important	No	No	2
			CVE-2023-29368	Elevation of Privilege	Important	No	No	2
5027230	高危	June 13, 2023— KB5027230 (OS Build	CVE-2023-32017	Remote Code Execution	Important	No	No	2
			CVE-2023-32015	Remote Code Execution	Critical	No	No	2

10240.19983) - Microsoft Support for Windows 10	CVE-2023-32030	Denial of Service	Important	No	No	2
	CVE-2023-29326	Remote Code Execution	Important	No	No	2
	CVE-2023-29364	Elevation of Privilege	Important	No	No	2
	CVE-2023-24897	Remote Code Execution	Critical	No	No	2
	CVE-2023-32014	Remote Code Execution	Critical	No	No	2
	CVE-2023-29370	Remote Code Execution	Important	No	No	2
	CVE-2023-29363	Remote Code Execution	Critical	No	No	2
	CVE-2023-29358	Elevation of Privilege	Important	No	No	1
	CVE-2023-29372	Remote Code Execution	Important	No	No	2
	CVE-2023-29351	Elevation of Privilege	Important	No	No	2
	CVE-2023-29373	Remote Code Execution	Important	No	No	2
	CVE-2023-29346	Elevation of Privilege	Important	No	No	2
	CVE-2023-32016	Information Disclosure	Important	No	No	2
	CVE-2023-32008	Remote Code Execution	Important	No	No	2
	CVE-2023-29365	Remote Code Execution	Important	No	No	2
	CVE-2023-24895	Remote Code Execution	Important	No	No	2
	CVE-2023-29359	Elevation of Privilege	Important	No	No	1
	CVE-2023-29371	Elevation of Privilege	Important	No	No	1
	CVE-2023-29362	Remote Code Execution	Important	No	No	2
	CVE-2023-24936	Elevation of Privilege	Moderate	No	No	2

			CVE-2023-32011	Denial of Service	Important	No	No	2
			CVE-2023-29331	Denial of Service	Important	No	No	2
			CVE-2023-29368	Elevation of Privilege	Important	No	No	2
5027271	高危	June 13, 2023—KB5027271 (Monthly Rollup) - Microsoft Support for Windows Server 2012 R2, Windows Embedded 8.1 Industry Enterprise, Windows Embedded 8.1 Industry Pro	CVE-2023-32017	Remote Code Execution	Important	No	No	2
			CVE-2023-32015	Remote Code Execution	Critical	No	No	2
			CVE-2023-29364	Elevation of Privilege	Important	No	No	2
			CVE-2023-32020	Spoofing	Important	No	No	2
			CVE-2023-32014	Remote Code Execution	Critical	No	No	2
			CVE-2023-29363	Remote Code Execution	Critical	No	No	2
			CVE-2023-29369	Denial of Service	Important	No	No	2
			CVE-2023-29367	Remote Code Execution	Important	No	No	2
			CVE-2023-29358	Elevation of Privilege	Important	No	No	1
			CVE-2023-29372	Remote Code Execution	Important	No	No	2
			CVE-2023-29351	Elevation of Privilege	Important	No	No	2
			CVE-2023-29373	Remote Code Execution	Important	No	No	2
			CVE-2023-29355	Information Disclosure	Important	No	No	2
			CVE-2023-29346	Elevation of Privilege	Important	No	No	2
			CVE-2023-32016	Information Disclosure	Important	No	No	2
			CVE-2023-32021	Security Feature Bypass	Important	No	No	2
CVE-2023-29365	Remote Code Execution	Important	No	No	2			

			CVE-2023-29359	Elevation of Privilege	Important	No	No	1
			CVE-2023-29371	Elevation of Privilege	Important	No	No	1
			CVE-2023-29362	Remote Code Execution	Important	No	No	2
			CVE-2023-32022	Security Feature Bypass	Important	No	No	2
			CVE-2023-32011	Denial of Service	Important	No	No	2
			CVE-2023-29368	Elevation of Privilege	Important	No	No	2
5027281	高危	June 13, 2023—KB5027281 (Security-only update) - Microsoft Support for Windows Server 2012, Windows Embedded 8 Standard	CVE-2023-32017	Remote Code Execution	Important	No	No	2
			CVE-2023-32015	Remote Code Execution	Critical	No	No	2
			CVE-2023-29364	Elevation of Privilege	Important	No	No	2
			CVE-2023-32020	Spoofing	Important	No	No	2
			CVE-2023-32014	Remote Code Execution	Critical	No	No	2
			CVE-2023-29363	Remote Code Execution	Critical	No	No	2
			CVE-2023-29369	Denial of Service	Important	No	No	2
			CVE-2023-29358	Elevation of Privilege	Important	No	No	1
			CVE-2023-29372	Remote Code Execution	Important	No	No	2
			CVE-2023-29351	Elevation of Privilege	Important	No	No	2
			CVE-2023-29373	Remote Code Execution	Important	No	No	2
			CVE-2023-29355	Information Disclosure	Important	No	No	2
			CVE-2023-29346	Elevation of Privilege	Important	No	No	2
			CVE-2023-32016	Information Disclosure	Important	No	No	2

			CVE-2023-29365	Remote Code Execution	Important	No	No	2
			CVE-2023-29359	Elevation of Privilege	Important	No	No	1
			CVE-2023-29371	Elevation of Privilege	Important	No	No	1
			CVE-2023-29362	Remote Code Execution	Important	No	No	2
			CVE-2023-32011	Denial of Service	Important	No	No	2
			CVE-2023-29368	Elevation of Privilege	Important	No	No	2
5027223	高危	June 13, 2023— KB5027223 (OS Build 22000.2057) – Microsoft Support for Windows 11 version 21H2, all editions	CVE-2023-32015	Remote Code Execution	Critical	No	No	2
			CVE-2023-32017	Remote Code Execution	Important	No	No	2
			CVE-2023-29366	Remote Code Execution	Important	No	No	2
			CVE-2023-29364	Elevation of Privilege	Important	No	No	2
			CVE-2023-29361	Elevation of Privilege	Important	No	No	1
			CVE-2023-32014	Remote Code Execution	Critical	No	No	2
			CVE-2023-29370	Remote Code Execution	Important	No	No	2
			CVE-2023-29363	Remote Code Execution	Critical	No	No	2
			CVE-2023-29358	Elevation of Privilege	Important	No	No	1
			CVE-2023-29372	Remote Code Execution	Important	No	No	2
			CVE-2023-29351	Elevation of Privilege	Important	No	No	2
			CVE-2023-29373	Remote Code Execution	Important	No	No	2
			CVE-2023-29360	Elevation of Privilege	Important	No	No	1
			CVE-2023-29346	Elevation of Privilege	Important	No	No	2

			CVE-2023-32016	Information Disclosure	Important	No	No	2
			CVE-2023-32019	Information Disclosure	Important	No	No	2
			CVE-2023-32008	Remote Code Execution	Important	No	No	2
			CVE-2023-29365	Remote Code Execution	Important	No	No	2
			CVE-2023-32012	Elevation of Privilege	Important	No	No	2
			CVE-2023-29359	Elevation of Privilege	Important	No	No	1
			CVE-2023-24937	Denial of Service	Important	No	No	2
			CVE-2023-24938	Denial of Service	Important	No	No	2
			CVE-2023-29352	Security Feature Bypass	Important	No	No	2
			CVE-2023-29371	Elevation of Privilege	Important	No	No	1
			CVE-2023-32013	Denial of Service	Critical	No	No	2
			CVE-2023-29362	Remote Code Execution	Important	No	No	2
			CVE-2023-32011	Denial of Service	Important	No	No	2
			CVE-2023-32009	Elevation of Privilege	Important	No	No	2
			CVE-2023-29368	Elevation of Privilege	Important	No	No	2

本月微软发布的软件安全更新补丁共 21 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
5027533	高危	June 13, 2023- Security Only Update for .NET Framework 3.5, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Windows Embedded 8.1 and Windows Server 2012 R2 (KB5027533) - Microsoft Support	CVE-2023-24936	Elevation of Privilege	Moderate	No	No	2
			CVE-2023-32030	Denial of Service	Important	No	No	2
			CVE-2023-24895	Remote Code Execution	Important	No	No	2
			CVE-2023-29326	Remote Code Execution	Important	No	No	2
			CVE-2023-24897	Remote Code Execution	Critical	No	No	2
			CVE-2023-29331	Denial of Service	Important	No	No	2
5027119	高危	June 13, 2023- KB5027119 Cumulative Update for .NET Framework 3.5 and 4.8.1 for Windows	CVE-2023-24936	Elevation of Privilege	Moderate	No	No	2
			CVE-2023-32030	Denial of Service	Important	No	No	2
			CVE-2023-24895	Remote Code Execution	Important	No	No	2
			CVE-2023-29326	Remote Code Execution	Important	No	No	2
			CVE-2023-24897	Remote Code Execution	Critical	No	No	2

		11, version 22H2 – Microsoft Support	CVE-2023-29331	Denial of Service	Important	No	No	2
5002405	高危	Description of the security update for Excel 2016: June 13, 2023 (KB5002405) – Microsoft Support	CVE-2023-33133	Remote Code Execution	Important	No	No	2
			CVE-2023-33137	Remote Code Execution	Important	No	No	2
			CVE-2023-32029	Remote Code Execution	Important	No	No	2
5027537	高危	June 13, 2023– KB5027537 Cumulative Update for .NET Framework 3.5, 4.8 and 4.8.1 for Windows 10 Version 21H2 – Microsoft Support	CVE-2023-24936	Elevation of Privilege	Moderate	No	No	2
			CVE-2023-32030	Denial of Service	Important	No	No	2
			CVE-2023-24895	Remote Code Execution	Important	No	No	2
			CVE-2023-29326	Remote Code Execution	Important	No	No	2
			CVE-2023-24897	Remote Code Execution	Critical	No	No	2
			CVE-2023-29331	Denial of Service	Important	No	No	2
5002414	高危	Description of the security update for Excel 2013: June 13, 2023 (KB500241	CVE-2023-33133	Remote Code Execution	Important	No	No	2
			CVE-2023-33137	Remote Code Execution	Important	No	No	2
			CVE-2023-32029	Remote Code Execution	Important	No	No	2

		4) - Microsoft Support						
5027539	高危	June 13, 2023- KB5027539 Cumulative Update for .NET Framework 3.5, 4.8 and 4.8.1 for Windows 11, version 21H2 - Microsoft Support	CVE-2023-24936	Elevation of Privilege	Moderate	No	No	2
			CVE-2023-32030	Denial of Service	Important	No	No	2
			CVE-2023-24895	Remote Code Execution	Important	No	No	2
			CVE-2023-29326	Remote Code Execution	Important	No	No	2
			CVE-2023-24897	Remote Code Execution	Critical	No	No	2
			CVE-2023-29331	Denial of Service	Important	No	No	2
5027536	高危	June 13, 2023- KB5027536 Cumulative Update for .NET Framework 3.5, 4.7.2 and 4.8 for Windows 10, version 1809 and Windows Server 2019 - Microsoft Support	CVE-2023-24936	Elevation of Privilege	Moderate	No	No	2
			CVE-2023-32030	Denial of Service	Important	No	No	2
			CVE-2023-24895	Remote Code Execution	Important	No	No	2
			CVE-2023-29326	Remote Code Execution	Important	No	No	2
			CVE-2023-24897	Remote Code Execution	Critical	No	No	2
			CVE-2023-29331	Denial of Service	Important	No	No	2
5027531	高危	June 13, 2023- Security Only	CVE-2023-24936	Elevation of Privilege	Moderate	No	No	2
			CVE-2023-32030	Denial of Service	Important	No	No	2

		Update for .NET Framework 3.5.1, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Windows Embedded 7 Standard and Windows Server 2008 R2 SP1 (KB5027531) - Microsoft Support	CVE-2023-24895	Remote Code Execution	Important	No	No	2
			CVE-2023-29326	Remote Code Execution	Important	No	No	2
			CVE-2023-24897	Remote Code Execution	Critical	No	No	2
			CVE-2023-29331	Denial of Service	Important	No	No	2
5027542	高危	June 13, 2023- Security and Quality Rollup for .NET Framework 3.5, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Windows Embedded 8.1 and Windows Server 2012 R2	CVE-2023-24936	Elevation of Privilege	Moderate	No	No	2
			CVE-2023-32030	Denial of Service	Important	No	No	2
			CVE-2023-24895	Remote Code Execution	Important	No	No	2
			CVE-2023-29326	Remote Code Execution	Important	No	No	2
			CVE-2023-24897	Remote Code Execution	Critical	No	No	2
			CVE-2023-29331	Denial of Service	Important	No	No	2

		(KB502754 2) - Microsoft Support						
5027540	高危	June 13, 2023- Security and Quality Rollup for .NET Framework 3.5.1, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Windows Embedded 7 Standard and Windows Server 2008 R2 SP1 (KB502754 0) - Microsoft Support	CVE-2023-24936	Elevation of Privilege	Moderate	No	No	2
			CVE-2023-32030	Denial of Service	Important	No	No	2
			CVE-2023-24895	Remote Code Execution	Important	No	No	2
			CVE-2023-29326	Remote Code Execution	Important	No	No	2
			CVE-2023-24897	Remote Code Execution	Critical	No	No	2
			CVE-2023-29331	Denial of Service	Important	No	No	2
5027544	高危	June 13, 2023- KB5027544 Cumulative Update for .NET Framework 3.5, 4.8 and 4.8.1 for	CVE-2023-24936	Elevation of Privilege	Moderate	No	No	2
			CVE-2023-32030	Denial of Service	Important	No	No	2
			CVE-2023-24895	Remote Code Execution	Important	No	No	2
			CVE-2023-29326	Remote Code Execution	Important	No	No	2
			CVE-2023-24897	Remote Code Execution	Critical	No	No	2

		Windows Server 2022 - Microsoft Support	CVE-2023-29331	Denial of Service	Important	No	No	2
5027538	高危	June 13, 2023-	CVE-2023-24936	Elevation of Privilege	Moderate	No	No	2
		KB5027538	CVE-2023-32030	Denial of Service	Important	No	No	2
		Cumulative Update for .NET Framework 3.5, 4.8 and 4.8.1 for Windows 10 Version 22H2 - Microsoft Support	CVE-2023-24895	Remote Code Execution	Important	No	No	2
			CVE-2023-29326	Remote Code Execution	Important	No	No	2
			CVE-2023-24897	Remote Code Execution	Critical	No	No	2
			CVE-2023-29331	Denial of Service	Important	No	No	2
5002404	高危	Description of the security update for SharePoint Enterprise Server 2016: June 13, 2023 (KB5002404) - Microsoft Support	CVE-2023-33129	Denial of Service	Important	No	No	2
5025903	高危	Description of the security update for	CVE-2023-28310	Remote Code Execution	Important	No	No	1
			CVE-2023-32031	Remote Code Execution	Important	No	No	1

		Microsoft Exchange Server 2016: June 13, 2023 (KB5025903) - Microsoft Support						
5027543	高危	June 13, 2023- Security and Quality Rollup for .NET Framework 2.0, 3.0, 4.6.2 for Windows Server 2008 SP2 (KB5027543) - Microsoft Support	CVE-2023-24936	Elevation of Privilege	Moderate	No	No	2
			CVE-2023-32030	Denial of Service	Important	No	No	2
			CVE-2023-24895	Remote Code Execution	Important	No	No	2
			CVE-2023-29326	Remote Code Execution	Important	No	No	2
			CVE-2023-24897	Remote Code Execution	Critical	No	No	2
			CVE-2023-29331	Denial of Service	Important	No	No	2
5027534	高危	June 13, 2023- Security Only Update for .NET Framework 2.0, 3.0, 4.6.2 for Windows Server 2008 SP2 (KB5027534) -	CVE-2023-24936	Elevation of Privilege	Moderate	No	No	2
			CVE-2023-32030	Denial of Service	Important	No	No	2
			CVE-2023-24895	Remote Code Execution	Important	No	No	2
			CVE-2023-29326	Remote Code Execution	Important	No	No	2
			CVE-2023-24897	Remote Code Execution	Critical	No	No	2
			CVE-2023-29331	Denial of Service	Important	No	No	2

		Microsoft Support						
5002387	高危	Description of the security update for Outlook 2016: June 13, 2023 (KB5002387) - Microsoft Support	CVE-2023-33131	Remote Code Execution	Important	No	No	2
5002382	高危	Description of the security update for Outlook 2013: June 13, 2023 (KB5002382) - Microsoft Support	CVE-2023-33131	Remote Code Execution	Important	No	No	2
5027541	高危	June 13, 2023- Security and Quality Rollup for .NET Framework 3.5, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for	CVE-2023-24936	Elevation of Privilege	Moderate	No	No	2
			CVE-2023-32030	Denial of Service	Important	No	No	2
			CVE-2023-24895	Remote Code Execution	Important	No	No	2
			CVE-2023-29326	Remote Code Execution	Important	No	No	2
			CVE-2023-24897	Remote Code Execution	Critical	No	No	2
			CVE-2023-29331	Denial of Service	Important	No	No	2

		Windows Embedded 8 Standard and Windows Server 2012 (KB5027541) - Microsoft Support						
5027123	高危	June 13, 2023- KB5027123 Cumulative Update for .NET Framework 4.8 for Windows 10, version 1607 and Windows Server 2016 - Microsoft Support	CVE-2023-24936	Elevation of Privilege	Moderate	No	No	2
			CVE-2023-32030	Denial of Service	Important	No	No	2
			CVE-2023-24895	Remote Code Execution	Important	No	No	2
			CVE-2023-24897	Remote Code Execution	Critical	No	No	2
			CVE-2023-29331	Denial of Service	Important	No	No	2
5027532	高危	June 13, 2023- Security Only Update for .NET Framework 3.5, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for	CVE-2023-24936	Elevation of Privilege	Moderate	No	No	2
			CVE-2023-32030	Denial of Service	Important	No	No	2
			CVE-2023-24895	Remote Code Execution	Important	No	No	2
			CVE-2023-29326	Remote Code Execution	Important	No	No	2
			CVE-2023-24897	Remote Code Execution	Critical	No	No	2
			CVE-2023-29331	Denial of Service	Important	No	No	2

		Windows Embedded 8 Standard and Windows Server 2012 (KB502753 2) - Microsoft Support						
--	--	--	--	--	--	--	--	--

本月发布内容 4 个一般性更新补丁。

KBID	奇安信集团级别	详细信息
4011621	其他功能性补丁	Office 2016 更新程序
5002308	其他功能性补丁	Office 2016 更新程序
5002343	其他功能性补丁	Office 2013 更新程序
5002349	其他功能性补丁	Office 2016 更新程序

注：

1、上述表格中“漏洞的可利用性”编号详细说明如下：

- 0 - 已被利用 (Exploitation Detected)
- 1 - 更有可能被利用 (Exploitation More Likely)
- 2 - 不太可能利用 (Exploitation Less Likely)
- 3 - 不可能利用 (Exploitation Unlikely)
- 4 - 不受漏洞的影响 (N/A)

第5章 参考链接

- Security Update Guide

<https://portal.msrc.microsoft.com/zh-cn/security-guidance>

- Latest non-security updates for versions of Office that use Windows Installer (MSI)

<https://docs.microsoft.com/en-us/OfficeUpdates/office-msi-non-security-updates>