奇安信集团 2023 年 8 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 8 月 9 日

目　录

文档信息

文档名称	奇安信集团 2023 年 8 月补丁库更新通告		
文档编号	Qi An Xin Group-MSPatch-2023-0801		
发布日期	2023-08-09	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:2023.08.09.1,V10版本:2023.08.09.1000)已发布，本次更新推送了50个微软安全补丁，修复了49个安全漏洞，其中4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、Internet Explorer、Office等产品。

第2章 重点关注补丁

本月有 18 个安全漏洞经奇安信评估满足以下任一条件，需要重点关注。

1. 漏洞等级（Severity）=严重（Critical），
2. 公开披露（Publicly Disclosed）=是（Yes），
3. 已受攻击（Exploited）=是（Yes），
4. 漏洞的可利用性（Exploitability Assessment）="已被利用（Exploitation Detected）" 或 "很可能被利用（Exploitation More Likely）"

详情如下：

KBID	修复的漏洞	漏洞的影响	漏洞等级	公开披露	已受攻击	漏洞的可利用性
5029301	CVE-2023-35359	Elevation of Privilege	Important	No	No	Exploitation More Likely
5029296						
5029247						
5029250						
5029318						
5029312						
5029259						
5029242						
5029307						
5029308						
5029304						
5029263						
5029295						
5029253						
5029244						
5029301	CVE-2023-36900	Elevation of Privilege	Important	No	No	Exploitation More Likely
5029296						
5029247						
5029250						
5029318						
5029312						
5029259						
5029242						
5029307						
5029308						
5029304						
5029263						
5029295						

5029253 5029244						
5029301 5029296 5029247 5029250 5029318 5029312 5029259 5029242 5029307 5029308 5029304 5029263 5029295 5029253 5029244	CVE-2023-35385	Remote Code Execution	Critical	No	No	Exploitation Less Likely
5029301 5029296 5029247 5029250 5029318 5029312 5029259 5029242 5029307 5029308 5029304 5029263 5029295 5029253 5029244	CVE-2023-36911	Remote Code Execution	Critical	No	No	Exploitation Less Likely
5029301 5029296 5029247 5029250 5029318 5029312 5029259 5029242 5029307	CVE-2023-35380	Elevation of Privilege	Important	No	No	Exploitation More Likely

5029308 5029304 5029263 5029295 5029253 5029244						
5029301 5029296 5029247 5029250 5029318 5029312 5029259 5029242 5029307 5029308 5029304 5029263 5029295 5029253 5029244	CVE-2023-36910	Remote Code Execution	Critical	No	No	Exploitation Less Likely
5002451 5002399 5002445 5002465 5002464 5002417 5002439 5002328 4504720 5002391 5002418 5002463 4484489 5002462	ADV230003	Defense in Depth	Moderate	Yes	Yes	Exploitation Detected
5029243 5029247 5029250 5029312 5029259 5029242	CVE-2023-35384	Security Feature Bypass	Important	No	No	Exploitation More Likely

5029304 5029263 5029253 5029244						
5002445 5002464	CVE-2023-36895	Remote Code Execution	Critical	No	No	Exploitation Less Likely
5029247 5029250 5029259 5029242 5029263 5029253 5029244	CVE-2023-35386	Elevation of Privilege	Important	No	No	Exploitation More Likely
5029247 5029250 5029263 5029253 5029244	CVE-2023-35382	Elevation of Privilege	Important	No	No	Exploitation More Likely
5029388	CVE-2023-35388	Remote Code Execution	Important	No	No	Exploitation More Likely
5029388	CVE-2023-38182	Remote Code Execution	Important	No	No	Exploitation More Likely

第3章 已知问题和特殊调整

本月暂无已知问题和特殊调整。

第4章 漏洞补丁详细列表

本月微软发布的系统安全更新补丁共 15 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
5029301	高危	August 8, 2023—KB5029301 (Security-only update) - Microsoft Support for Windows Server 2008 Datacenter ESU,Windows Server 2008 Standard ESU,Windows Server 2008 Enterprise ESU	CVE-2023-36906	Information Disclosure	Important	No	No	2
			CVE-2023-38184	Remote Code Execution	Important	No	No	2
			CVE-2023-35376	Denial of Service	Important	No	No	2
			CVE-2023-38172	Denial of Service	Important	No	No	2
			CVE-2023-35383	Information Disclosure	Important	No	No	2
			CVE-2023-20569	Information Disclosure	Important	No	No	2
			CVE-2023-36913	Information Disclosure	Important	No	No	2
			CVE-2023-35359	Elevation of Privilege	Important	No	No	1
			CVE-2023-38254	Denial of Service	Important	No	No	2
			CVE-2023-36912	Denial of Service	Important	No	No	2
			CVE-2023-36900	Elevation of Privilege	Important	No	No	1
			CVE-2023-35385	Remote Code Execution	Critical	No	No	2
			CVE-2023-36911	Remote Code Execution	Critical	No	No	2
			CVE-2023-36882	Remote Code Execution	Important	No	No	2
			CVE-2023-36909	Denial of Service	Important	No	No	2

			CVE-2023-36889	Security Feature Bypass	Important	No	No	2
			CVE-2023-35377	Denial of Service	Important	No	No	2
			CVE-2023-35380	Elevation of Privilege	Important	No	No	1
			CVE-2023-36910	Remote Code Execution	Critical	No	No	2
			CVE-2023-35381	Remote Code Execution	Important	No	No	2
			CVE-2023-36907	Information Disclosure	Important	No	No	2
5029296	高危	August 8, 2023—KB5029296 (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,Windo	CVE-2023-36906	Information Disclosure	Important	No	No	2
			CVE-2023-38184	Remote Code Execution	Important	No	No	2
			CVE-2023-35376	Denial of Service	Important	No	No	2
			CVE-2023-38172	Denial of Service	Important	No	No	2
			CVE-2023-35383	Information Disclosure	Important	No	No	2
			CVE-2023-20569	Information Disclosure	Important	No	No	2
			CVE-2023-36913	Information Disclosure	Important	No	No	2
			CVE-2023-36903	Elevation of Privilege	Important	No	No	2
			CVE-2023-35359	Elevation of Privilege	Important	No	No	1
			CVE-2023-35379	Elevation of Privilege	Important	No	No	2
			CVE-2023-38254	Denial of Service	Important	No	No	2
			CVE-2023-36912	Denial of Service	Important	No	No	2
			CVE-2023-36900	Elevation of Privilege	Important	No	No	1
			CVE-2023-36908	Information Disclosure	Important	No	No	2

		ws Embedded POSReady 7 ESU	CVE-2023-36876	Elevation of Privilege	Important	No	No	2
			CVE-2023-35385	Remote Code Execution	Critical	No	No	2
			CVE-2023-36911	Remote Code Execution	Critical	No	No	2
			CVE-2023-36882	Remote Code Execution	Important	No	No	2
			CVE-2023-36909	Denial of Service	Important	No	No	2
			CVE-2023-36889	Security Feature Bypass	Important	No	No	2
			CVE-2023-35377	Denial of Service	Important	No	No	2
			CVE-2023-35380	Elevation of Privilege	Important	No	No	1
			CVE-2023-36910	Remote Code Execution	Critical	No	No	2
			CVE-2023-35381	Remote Code Execution	Important	No	No	2
			CVE-2023-36907	Information Disclosure	Important	No	No	2
5029247	高危	August 8, 2023—KB5029247 (OS Build 17763.4737) - Microsoft Support for Win 10 Ent LTSC v2019,Win 10 IoT Ent LTSC v2019,Windows 10 IoT Core 2019	CVE-2023-36904	Elevation of Privilege	Important	No	No	2
			CVE-2023-36906	Information Disclosure	Important	No	No	2
			CVE-2023-38184	Remote Code Execution	Important	No	No	2
			CVE-2023-35376	Denial of Service	Important	No	No	2
			CVE-2023-38172	Denial of Service	Important	No	No	2
			CVE-2023-36907	Information Disclosure	Important	No	No	2
			CVE-2023-35383	Information Disclosure	Important	No	No	2
			CVE-2023-20569	Information Disclosure	Important	No	No	2
			CVE-2023-36913	Information Disclosure	Important	No	No	2

		LTSC,Windows Server 2019	CVE-2023-36903	Elevation of Privilege	Important	No	No	2
			CVE-2023-35384	Security Feature Bypass	Important	No	No	1
			CVE-2023-35359	Elevation of Privilege	Important	No	No	1
			CVE-2023-36905	Information Disclosure	Important	No	No	2
			CVE-2023-38254	Denial of Service	Important	No	No	2
			CVE-2023-36912	Denial of Service	Important	No	No	2
			CVE-2023-36900	Elevation of Privilege	Important	No	No	1
			CVE-2023-36908	Information Disclosure	Important	No	No	2
			CVE-2023-35385	Remote Code Execution	Critical	No	No	2
			CVE-2023-35378	Elevation of Privilege	Important	No	No	2
			CVE-2023-36911	Remote Code Execution	Critical	No	No	2
			CVE-2023-36882	Remote Code Execution	Important	No	No	2
			CVE-2023-36909	Denial of Service	Important	No	No	2
			CVE-2023-35387	Elevation of Privilege	Important	No	No	2
			CVE-2023-36889	Security Feature Bypass	Important	No	No	2
			CVE-2023-35377	Denial of Service	Important	No	No	2
			CVE-2023-38154	Elevation of Privilege	Important	No	No	3
			CVE-2023-35380	Elevation of Privilege	Important	No	No	1
			CVE-2023-35386	Elevation of Privilege	Important	No	No	1

			CVE-2023-36910	Remote Code Execution	Critical	No	No	2
			CVE-2023-35381	Remote Code Execution	Important	No	No	2
			CVE-2023-35382	Elevation of Privilege	Important	No	No	1
5029250	高危	August 8, 2023—KB5029250 (OS Build 20348.1906) - Microsoft Support for Windows Server 2022	CVE-2023-36904	Elevation of Privilege	Important	No	No	2
			CVE-2023-36906	Information Disclosure	Important	No	No	2
			CVE-2023-38184	Remote Code Execution	Important	No	No	2
			CVE-2023-35376	Denial of Service	Important	No	No	2
			CVE-2023-38172	Denial of Service	Important	No	No	2
			CVE-2023-36907	Information Disclosure	Important	No	No	2
			CVE-2023-35383	Information Disclosure	Important	No	No	2
			CVE-2023-20569	Information Disclosure	Important	No	No	2
			CVE-2023-36913	Information Disclosure	Important	No	No	2
			CVE-2023-36903	Elevation of Privilege	Important	No	No	2
			CVE-2023-35384	Security Feature Bypass	Important	No	No	1
			CVE-2023-35359	Elevation of Privilege	Important	No	No	1
			CVE-2023-38254	Denial of Service	Important	No	No	2
			CVE-2023-36912	Denial of Service	Important	No	No	2
			CVE-2023-36900	Elevation of Privilege	Important	No	No	1
			CVE-2023-38186	Elevation of Privilege	Important	No	No	2
			CVE-2023-36908	Information Disclosure	Important	No	No	2

			CVE-2023-35385	Remote Code Execution	Critical	No	No	2
			CVE-2023-35378	Elevation of Privilege	Important	No	No	2
			CVE-2023-36911	Remote Code Execution	Critical	No	No	2
			CVE-2023-36914	Security Feature Bypass	Important	No	No	2
			CVE-2023-36882	Remote Code Execution	Important	No	No	2
			CVE-2023-36909	Denial of Service	Important	No	No	2
			CVE-2023-36889	Security Feature Bypass	Important	No	No	2
			CVE-2023-35377	Denial of Service	Important	No	No	2
			CVE-2023-35380	Elevation of Privilege	Important	No	No	1
			CVE-2023-35386	Elevation of Privilege	Important	No	No	1
			CVE-2023-36910	Remote Code Execution	Critical	No	No	2
			CVE-2023-35381	Remote Code Execution	Important	No	No	2
			CVE-2023-35382	Elevation of Privilege	Important	No	No	1
5029318	高危	August 8, 2023—KB5029318 (Monthly Rollup) - Microsoft Support for Windows Server 2008 Datacente	CVE-2023-36906	Information Disclosure	Important	No	No	2
			CVE-2023-38184	Remote Code Execution	Important	No	No	2
			CVE-2023-35376	Denial of Service	Important	No	No	2
			CVE-2023-38172	Denial of Service	Important	No	No	2
			CVE-2023-35383	Information Disclosure	Important	No	No	2
			CVE-2023-20569	Information Disclosure	Important	No	No	2

		r ESU,Windows Server 2008 Standard ESU,Windows Server 2008 Enterprise ESU	CVE-2023-36913	Information Disclosure	Important	No	No	2
			CVE-2023-35359	Elevation of Privilege	Important	No	No	1
			CVE-2023-38254	Denial of Service	Important	No	No	2
			CVE-2023-36912	Denial of Service	Important	No	No	2
			CVE-2023-36900	Elevation of Privilege	Important	No	No	1
			CVE-2023-35385	Remote Code Execution	Critical	No	No	2
			CVE-2023-36911	Remote Code Execution	Critical	No	No	2
			CVE-2023-36882	Remote Code Execution	Important	No	No	2
			CVE-2023-36909	Denial of Service	Important	No	No	2
			CVE-2023-36889	Security Feature Bypass	Important	No	No	2
			CVE-2023-35377	Denial of Service	Important	No	No	2
			CVE-2023-35380	Elevation of Privilege	Important	No	No	1
			CVE-2023-36910	Remote Code Execution	Critical	No	No	2
			CVE-2023-35381	Remote Code Execution	Important	No	No	2
			CVE-2023-36907	Information Disclosure	Important	No	No	2
5029312	高危	August 8, 2023—KB5029312 (Monthly Rollup) - Microsoft Support for Windows	CVE-2023-36906	Information Disclosure	Important	No	No	2
			CVE-2023-38184	Remote Code Execution	Important	No	No	2
			CVE-2023-35376	Denial of Service	Important	No	No	2
			CVE-2023-38172	Denial of Service	Important	No	No	2
			CVE-2023-35383	Information Disclosure	Important	No	No	2

		Server 2012 R2	CVE-2023-20569	Information Disclosure	Important	No	No	2
			CVE-2023-36913	Information Disclosure	Important	No	No	2
			CVE-2023-36903	Elevation of Privilege	Important	No	No	2
			CVE-2023-35384	Security Feature Bypass	Important	No	No	1
			CVE-2023-35359	Elevation of Privilege	Important	No	No	1
			CVE-2023-38254	Denial of Service	Important	No	No	2
			CVE-2023-36912	Denial of Service	Important	No	No	2
			CVE-2023-36900	Elevation of Privilege	Important	No	No	1
			CVE-2023-36908	Information Disclosure	Important	No	No	2
			CVE-2023-35385	Remote Code Execution	Critical	No	No	2
			CVE-2023-36911	Remote Code Execution	Critical	No	No	2
			CVE-2023-36882	Remote Code Execution	Important	No	No	2
			CVE-2023-36909	Denial of Service	Important	No	No	2
			CVE-2023-35387	Elevation of Privilege	Important	No	No	2
			CVE-2023-36889	Security Feature Bypass	Important	No	No	2
			CVE-2023-35377	Denial of Service	Important	No	No	2
			CVE-2023-35380	Elevation of Privilege	Important	No	No	1
			CVE-2023-36910	Remote Code Execution	Critical	No	No	2
			CVE-2023-35381	Remote Code Execution	Important	No	No	2

			CVE-2023-36907	Information Disclosure	Important	No	No	2
5029259	高危	August 8, 2023—KB5029259 (OS Build 10240.20107) - Microsoft Support for Windows 10	CVE-2023-36906	Information Disclosure	Important	No	No	2
			CVE-2023-38184	Remote Code Execution	Important	No	No	2
			CVE-2023-35376	Denial of Service	Important	No	No	2
			CVE-2023-38172	Denial of Service	Important	No	No	2
			CVE-2023-35383	Information Disclosure	Important	No	No	2
			CVE-2023-20569	Information Disclosure	Important	No	No	2
			CVE-2023-36913	Information Disclosure	Important	No	No	2
			CVE-2023-36903	Elevation of Privilege	Important	No	No	2
			CVE-2023-35384	Security Feature Bypass	Important	No	No	1
			CVE-2023-35359	Elevation of Privilege	Important	No	No	1
			CVE-2023-36905	Information Disclosure	Important	No	No	2
			CVE-2023-38254	Denial of Service	Important	No	No	2
			CVE-2023-36912	Denial of Service	Important	No	No	2
			CVE-2023-36900	Elevation of Privilege	Important	No	No	1
			CVE-2023-36908	Information Disclosure	Important	No	No	2
			CVE-2023-35385	Remote Code Execution	Critical	No	No	2
			CVE-2023-36911	Remote Code Execution	Critical	No	No	2
			CVE-2023-36882	Remote Code Execution	Important	No	No	2
			CVE-2023-36909	Denial of Service	Important	No	No	2

			CVE-2023-35387	Elevation of Privilege	Important	No	No	2
			CVE-2023-36889	Security Feature Bypass	Important	No	No	2
			CVE-2023-35377	Denial of Service	Important	No	No	2
			CVE-2023-35380	Elevation of Privilege	Important	No	No	1
			CVE-2023-35386	Elevation of Privilege	Important	No	No	1
			CVE-2023-36910	Remote Code Execution	Critical	No	No	2
			CVE-2023-35381	Remote Code Execution	Important	No	No	2
			CVE-2023-36907	Information Disclosure	Important	No	No	2
5029242	高危	August 8, 2023—KB5029242 (OS Build 14393.6167) - Microsoft Support for Windows 10, version 1607, all editions, Windows Server 2016, all editions	CVE-2023-36906	Information Disclosure	Important	No	No	2
			CVE-2023-38184	Remote Code Execution	Important	No	No	2
			CVE-2023-35376	Denial of Service	Important	No	No	2
			CVE-2023-38172	Denial of Service	Important	No	No	2
			CVE-2023-35383	Information Disclosure	Important	No	No	2
			CVE-2023-20569	Information Disclosure	Important	No	No	2
			CVE-2023-36913	Information Disclosure	Important	No	No	2
			CVE-2023-36903	Elevation of Privilege	Important	No	No	2
			CVE-2023-35384	Security Feature Bypass	Important	No	No	1
			CVE-2023-35359	Elevation of Privilege	Important	No	No	1
			CVE-2023-36905	Information Disclosure	Important	No	No	2

			CVE-2023-38254	Denial of Service	Important	No	No	2
			CVE-2023-36912	Denial of Service	Important	No	No	2
			CVE-2023-36900	Elevation of Privilege	Important	No	No	1
			CVE-2023-36908	Information Disclosure	Important	No	No	2
			CVE-2023-35385	Remote Code Execution	Critical	No	No	2
			CVE-2023-36911	Remote Code Execution	Critical	No	No	2
			CVE-2023-36882	Remote Code Execution	Important	No	No	2
			CVE-2023-36909	Denial of Service	Important	No	No	2
			CVE-2023-35387	Elevation of Privilege	Important	No	No	2
			CVE-2023-36889	Security Feature Bypass	Important	No	No	2
			CVE-2023-35377	Denial of Service	Important	No	No	2
			CVE-2023-35380	Elevation of Privilege	Important	No	No	1
			CVE-2023-35386	Elevation of Privilege	Important	No	No	1
			CVE-2023-36910	Remote Code Execution	Critical	No	No	2
			CVE-2023-35381	Remote Code Execution	Important	No	No	2
			CVE-2023-36907	Information Disclosure	Important	No	No	2
5029307	高危	August 8, 2023—KB5029307 (Security-only update) - Microsoft Support	CVE-2023-36906	Information Disclosure	Important	No	No	2
			CVE-2023-38184	Remote Code Execution	Important	No	No	2
			CVE-2023-35376	Denial of Service	Important	No	No	2
			CVE-2023-38172	Denial of Service	Important	No	No	2

		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-2023-35383	Information Disclosure	Important	No	No	2
			CVE-2023-20569	Information Disclosure	Important	No	No	2
			CVE-2023-36913	Information Disclosure	Important	No	No	2
			CVE-2023-36903	Elevation of Privilege	Important	No	No	2
			CVE-2023-35359	Elevation of Privilege	Important	No	No	1
			CVE-2023-35379	Elevation of Privilege	Important	No	No	2
			CVE-2023-38254	Denial of Service	Important	No	No	2
			CVE-2023-36912	Denial of Service	Important	No	No	2
			CVE-2023-36900	Elevation of Privilege	Important	No	No	1
			CVE-2023-36908	Information Disclosure	Important	No	No	2
			CVE-2023-36876	Elevation of Privilege	Important	No	No	2
			CVE-2023-35385	Remote Code Execution	Critical	No	No	2
			CVE-2023-36911	Remote Code Execution	Critical	No	No	2
			CVE-2023-36882	Remote Code Execution	Important	No	No	2
			CVE-2023-36909	Denial of Service	Important	No	No	2
			CVE-2023-36889	Security Feature Bypass	Important	No	No	2
			CVE-2023-35377	Denial of Service	Important	No	No	2
			CVE-2023-35380	Elevation of Privilege	Important	No	No	1
			CVE-2023-36910	Remote Code Execution	Critical	No	No	2
			CVE-2023-35381	Remote Code Execution	Important	No	No	2

			CVE-2023-36907	Information Disclosure	Important	No	No	2
5029308	高危	August 8, 2023—KB5029308 (Security-only update) - Microsoft Support for Windows Server 2012	CVE-2023-36906	Information Disclosure	Important	No	No	2
			CVE-2023-38184	Remote Code Execution	Important	No	No	2
			CVE-2023-35376	Denial of Service	Important	No	No	2
			CVE-2023-38172	Denial of Service	Important	No	No	2
			CVE-2023-35383	Information Disclosure	Important	No	No	2
			CVE-2023-20569	Information Disclosure	Important	No	No	2
			CVE-2023-36913	Information Disclosure	Important	No	No	2
			CVE-2023-36903	Elevation of Privilege	Important	No	No	2
			CVE-2023-35359	Elevation of Privilege	Important	No	No	1
			CVE-2023-38254	Denial of Service	Important	No	No	2
			CVE-2023-36912	Denial of Service	Important	No	No	2
			CVE-2023-36900	Elevation of Privilege	Important	No	No	1
			CVE-2023-36908	Information Disclosure	Important	No	No	2
			CVE-2023-35385	Remote Code Execution	Critical	No	No	2
			CVE-2023-36911	Remote Code Execution	Critical	No	No	2
			CVE-2023-36882	Remote Code Execution	Important	No	No	2
			CVE-2023-36909	Denial of Service	Important	No	No	2
			CVE-2023-35387	Elevation of Privilege	Important	No	No	2
			CVE-2023-36889	Security Feature Bypass	Important	No	No	2

			CVE-2023-35377	Denial of Service	Important	No	No	2
			CVE-2023-35380	Elevation of Privilege	Important	No	No	1
			CVE-2023-36910	Remote Code Execution	Critical	No	No	2
			CVE-2023-35381	Remote Code Execution	Important	No	No	2
			CVE-2023-36907	Information Disclosure	Important	No	No	2
5029304	高危	August 8, 2023—KB5029304 (Security-only update) - Microsoft Support for Windows Server 2012 R2	CVE-2023-36906	Information Disclosure	Important	No	No	2
			CVE-2023-38184	Remote Code Execution	Important	No	No	2
			CVE-2023-35376	Denial of Service	Important	No	No	2
			CVE-2023-38172	Denial of Service	Important	No	No	2
			CVE-2023-35383	Information Disclosure	Important	No	No	2
			CVE-2023-20569	Information Disclosure	Important	No	No	2
			CVE-2023-36913	Information Disclosure	Important	No	No	2
			CVE-2023-36903	Elevation of Privilege	Important	No	No	2
			CVE-2023-35384	Security Feature Bypass	Important	No	No	1
			CVE-2023-35359	Elevation of Privilege	Important	No	No	1
			CVE-2023-38254	Denial of Service	Important	No	No	2
			CVE-2023-36912	Denial of Service	Important	No	No	2
			CVE-2023-36900	Elevation of Privilege	Important	No	No	1
			CVE-2023-36908	Information Disclosure	Important	No	No	2
			CVE-2023-35385	Remote Code Execution	Critical	No	No	2

			CVE-2023-36911	Remote Code Execution	Critical	No	No	2
			CVE-2023-36882	Remote Code Execution	Important	No	No	2
			CVE-2023-36909	Denial of Service	Important	No	No	2
			CVE-2023-35387	Elevation of Privilege	Important	No	No	2
			CVE-2023-36889	Security Feature Bypass	Important	No	No	2
			CVE-2023-35377	Denial of Service	Important	No	No	2
			CVE-2023-35380	Elevation of Privilege	Important	No	No	1
			CVE-2023-36910	Remote Code Execution	Critical	No	No	2
			CVE-2023-35381	Remote Code Execution	Important	No	No	2
			CVE-2023-36907	Information Disclosure	Important	No	No	2
5029263	高危	August 8, 2023—KB5029263 (OS Build 22621.2134) - Microsoft Support for Windows 11 version 22H2, all editions	CVE-2023-36904	Elevation of Privilege	Important	No	No	2
			CVE-2023-36906	Information Disclosure	Important	No	No	2
			CVE-2023-38184	Remote Code Execution	Important	No	No	2
			CVE-2023-35376	Denial of Service	Important	No	No	2
			CVE-2023-38172	Denial of Service	Important	No	No	2
			CVE-2023-36907	Information Disclosure	Important	No	No	2
			CVE-2023-35383	Information Disclosure	Important	No	No	2
			CVE-2023-20569	Information Disclosure	Important	No	No	2
			CVE-2023-36913	Information Disclosure	Important	No	No	2
			CVE-2023-36903	Elevation of Privilege	Important	No	No	2

			CVE-2023-35384	Security Feature Bypass	Important	No	No	1
			CVE-2023-35359	Elevation of Privilege	Important	No	No	1
			CVE-2023-36905	Information Disclosure	Important	No	No	2
			CVE-2023-38254	Denial of Service	Important	No	No	2
			CVE-2023-36912	Denial of Service	Important	No	No	2
			CVE-2023-36900	Elevation of Privilege	Important	No	No	1
			CVE-2023-38186	Elevation of Privilege	Important	No	No	2
			CVE-2023-36908	Information Disclosure	Important	No	No	2
			CVE-2023-36898	Remote Code Execution	Important	No	No	2
			CVE-2023-35385	Remote Code Execution	Critical	No	No	2
			CVE-2023-35378	Elevation of Privilege	Important	No	No	2
			CVE-2023-36911	Remote Code Execution	Critical	No	No	2
			CVE-2023-36914	Security Feature Bypass	Important	No	No	2
			CVE-2023-36882	Remote Code Execution	Important	No	No	2
			CVE-2023-36909	Denial of Service	Important	No	No	2
			CVE-2023-36889	Security Feature Bypass	Important	No	No	2
			CVE-2023-35387	Elevation of Privilege	Important	No	No	2
			CVE-2023-35377	Denial of Service	Important	No	No	2
			CVE-2023-35380	Elevation of Privilege	Important	No	No	1

			CVE-2023-35386	Elevation of Privilege	Important	No	No	1
			CVE-2023-36910	Remote Code Execution	Critical	No	No	2
			CVE-2023-35381	Remote Code Execution	Important	No	No	2
			CVE-2023-35382	Elevation of Privilege	Important	No	No	1
5029295	高危	August 8, 2023—KB5029295 (Monthly Rollup) - Microsoft Support for Windows Server 2012	CVE-2023-36906	Information Disclosure	Important	No	No	2
			CVE-2023-38184	Remote Code Execution	Important	No	No	2
			CVE-2023-35376	Denial of Service	Important	No	No	2
			CVE-2023-38172	Denial of Service	Important	No	No	2
			CVE-2023-35383	Information Disclosure	Important	No	No	2
			CVE-2023-20569	Information Disclosure	Important	No	No	2
			CVE-2023-36913	Information Disclosure	Important	No	No	2
			CVE-2023-36903	Elevation of Privilege	Important	No	No	2
			CVE-2023-35359	Elevation of Privilege	Important	No	No	1
			CVE-2023-38254	Denial of Service	Important	No	No	2
			CVE-2023-36912	Denial of Service	Important	No	No	2
			CVE-2023-36900	Elevation of Privilege	Important	No	No	1
			CVE-2023-36908	Information Disclosure	Important	No	No	2
			CVE-2023-35385	Remote Code Execution	Critical	No	No	2
			CVE-2023-36911	Remote Code Execution	Critical	No	No	2
			CVE-2023-36882	Remote Code Execution	Important	No	No	2

			CVE-2023-36909	Denial of Service	Important	No	No	2
			CVE-2023-35387	Elevation of Privilege	Important	No	No	2
			CVE-2023-36889	Security Feature Bypass	Important	No	No	2
			CVE-2023-35377	Denial of Service	Important	No	No	2
			CVE-2023-35380	Elevation of Privilege	Important	No	No	1
			CVE-2023-36910	Remote Code Execution	Critical	No	No	2
			CVE-2023-35381	Remote Code Execution	Important	No	No	2
			CVE-2023-36907	Information Disclosure	Important	No	No	2
5029253	高危	August 8, 2023—KB5029253 (OS Build 22000.2295) - Microsoft Support for Windows 11 version 21H2, all editions	CVE-2023-36904	Elevation of Privilege	Important	No	No	2
			CVE-2023-36906	Information Disclosure	Important	No	No	2
			CVE-2023-38184	Remote Code Execution	Important	No	No	2
			CVE-2023-35376	Denial of Service	Important	No	No	2
			CVE-2023-38172	Denial of Service	Important	No	No	2
			CVE-2023-36907	Information Disclosure	Important	No	No	2
			CVE-2023-35383	Information Disclosure	Important	No	No	2
			CVE-2023-20569	Information Disclosure	Important	No	No	2
			CVE-2023-36913	Information Disclosure	Important	No	No	2
			CVE-2023-36903	Elevation of Privilege	Important	No	No	2
			CVE-2023-35384	Security Feature Bypass	Important	No	No	1

			CVE-2023-35359	Elevation of Privilege	Important	No	No	1
			CVE-2023-36905	Information Disclosure	Important	No	No	2
			CVE-2023-38254	Denial of Service	Important	No	No	2
			CVE-2023-36912	Denial of Service	Important	No	No	2
			CVE-2023-36900	Elevation of Privilege	Important	No	No	1
			CVE-2023-38186	Elevation of Privilege	Important	No	No	2
			CVE-2023-36908	Information Disclosure	Important	No	No	2
			CVE-2023-36898	Remote Code Execution	Important	No	No	2
			CVE-2023-35385	Remote Code Execution	Critical	No	No	2
			CVE-2023-35378	Elevation of Privilege	Important	No	No	2
			CVE-2023-36911	Remote Code Execution	Critical	No	No	2
			CVE-2023-36914	Security Feature Bypass	Important	No	No	2
			CVE-2023-36882	Remote Code Execution	Important	No	No	2
			CVE-2023-36909	Denial of Service	Important	No	No	2
			CVE-2023-36889	Security Feature Bypass	Important	No	No	2
			CVE-2023-35387	Elevation of Privilege	Important	No	No	2
			CVE-2023-35377	Denial of Service	Important	No	No	2
			CVE-2023-35380	Elevation of Privilege	Important	No	No	1
			CVE-2023-35386	Elevation of Privilege	Important	No	No	1

			CVE-2023-36910	Remote Code Execution	Critical	No	No	2
			CVE-2023-35381	Remote Code Execution	Important	No	No	2
			CVE-2023-35382	Elevation of Privilege	Important	No	No	1
5029244	高危	August 8, 2023—KB5029244 (OS Builds 19044.3324 and 19045.3324) - Microsoft Support for Windows 10 Enterprise and Education, version 21H2,Windows 10 IoT Enterprise, version 21H2,Windows 10 Enterprise Multi-Session, version 21H2,Windows 10, version 22H2, all editions	CVE-2023-36904	Elevation of Privilege	Important	No	No	2
			CVE-2023-36906	Information Disclosure	Important	No	No	2
			CVE-2023-38184	Remote Code Execution	Important	No	No	2
			CVE-2023-35376	Denial of Service	Important	No	No	2
			CVE-2023-38172	Denial of Service	Important	No	No	2
			CVE-2023-36907	Information Disclosure	Important	No	No	2
			CVE-2023-35383	Information Disclosure	Important	No	No	2
			CVE-2023-20569	Information Disclosure	Important	No	No	2
			CVE-2023-36913	Information Disclosure	Important	No	No	2
			CVE-2023-36903	Elevation of Privilege	Important	No	No	2
			CVE-2023-35384	Security Feature Bypass	Important	No	No	1
			CVE-2023-35359	Elevation of Privilege	Important	No	No	1
			CVE-2023-36905	Information Disclosure	Important	No	No	2
			CVE-2023-38254	Denial of Service	Important	No	No	2
			CVE-2023-36912	Denial of Service	Important	No	No	2
			CVE-2023-36900	Elevation of Privilege	Important	No	No	1
			CVE-2023-38186	Elevation of Privilege	Important	No	No	2

			CVE-2023-36908	Information Disclosure	Important	No	No	2
			CVE-2023-35385	Remote Code Execution	Critical	No	No	2
			CVE-2023-35378	Elevation of Privilege	Important	No	No	2
			CVE-2023-36911	Remote Code Execution	Critical	No	No	2
			CVE-2023-36914	Security Feature Bypass	Important	No	No	2
			CVE-2023-36882	Remote Code Execution	Important	No	No	2
			CVE-2023-36909	Denial of Service	Important	No	No	2
			CVE-2023-35387	Elevation of Privilege	Important	No	No	2
			CVE-2023-36889	Security Feature Bypass	Important	No	No	2
			CVE-2023-35377	Denial of Service	Important	No	No	2
			CVE-2023-35380	Elevation of Privilege	Important	No	No	1
			CVE-2023-35386	Elevation of Privilege	Important	No	No	1
			CVE-2023-36910	Remote Code Execution	Critical	No	No	2
			CVE-2023-35381	Remote Code Execution	Important	No	No	2
			CVE-2023-35382	Elevation of Privilege	Important	No	No	1

本月微软发布的软件安全更新补丁共 35 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
5002398	高危	Description of the security update for SharePoint Enterprise Server 2016 Language Pack: August 8, 2023 (KB5002398) - Microsoft Support	CVE-2023-36894	Information Disclosure	Important	No	No	2
5029650	高危	August 8, 2023-KB5029650 Cumulative Update for .NET Framework 3.5, 4.8 and 4.8.1 for Windows 11, version 21H2 -	CVE-2023-36899	Elevation of Privilege	Important	No	No	2
			CVE-2023-36873	Spoofing	Important	No	No	2

		Microsoft Support						
5002451	高危	Description of the security update for Excel 2013: August 8, 2023 (KB5002451) - Microsoft Support	CVE-2023-36896	Remote Code Execution	Important	No	No	2
			ADV230003	Defense in Depth	Moderate	Yes	Yes	0
5029243	高危	KB5029243: Cumulative security update for Internet Explorer: August 8, 2023 - Microsoft Support	CVE-2023-35384	Security Feature Bypass	Important	No	No	1
5029647	高危	August 8, 2023-KB5029647 Cumulative Update for .NET Framework 3.5, 4.7.2 and 4.8 for Windows 10, version 1809 and Windows	CVE-2023-36899	Elevation of Privilege	Important	No	No	2
			CVE-2023-36873	Spoofing	Important	No	No	2

		Server 2019 - Microsoft Support						
5002399	高危	Description of the security update for PowerPoint 2013: August 8, 2023 (KB5002399) - Microsoft Support	ADV230003	Defense in Depth	Moderate	Yes	Yes	0
5002445	高危	Description of the security update for Word 2013: August 8, 2023 (KB5002445) - Microsoft Support	CVE-2023-36895	Remote Code Execution	Critical	No	No	2
			ADV230003	Defense in Depth	Moderate	Yes	Yes	0
5002449	高危	Description of the security update for Outlook 2013: August 8, 2023 (KB5002449) - Microsoft Support	CVE-2023-36893	Spoofing	Important	No	No	2

5002465	高危	Description of the security update for Office 2016: August 8, 2023 (KB5002465) - Microsoft Support	ADV230003	Defense in Depth	Moderate	Yes	Yes	0
5002464	高危	Description of the security update for Word 2016: August 8, 2023 (KB5002464) - Microsoft Support	CVE-2023-36895	Remote Code Execution	Critical	No	No	2
			ADV230003	Defense in Depth	Moderate	Yes	Yes	0
5002417	高危	Description of the security update for Visio 2013: August 8, 2023 (KB5002417) - Microsoft Support	ADV230003	Defense in Depth	Moderate	Yes	Yes	0
5002459	高危	Description of the security update for	CVE-2023-36893	Spoofing	Important	No	No	2

		Outlook 2016: August 8, 2023 (KB5002459) - Microsoft Support						
5002439	高危	Description of the security update for Office 2013: August 8, 2023 (KB5002439) - Microsoft Support	ADV230003	Defense in Depth	Moderate	Yes	Yes	0
5029388	高危	Description of the security update for Microsoft Exchange Server 2019 and 2016: August 8, 2023 (KB5029388) - Microsoft Support	CVE-2023-35388	Remote Code Execution	Important	No	No	1
			CVE-2023-38185	Remote Code Execution	Important	No	No	2
			CVE-2023-38182	Remote Code Execution	Important	No	No	1
			CVE-2023-35368	Remote Code Execution	Important	No	No	2
			CVE-2023-21709	Elevation of Privilege	Important	No	No	2
			CVE-2023-38181	Spoofing	Important	No	No	2
5002453	高危	Description of the security update for	CVE-2023-36894	Information Disclosure	Important	No	No	2

		SharePoint Enterprise Server 2016: August 8, 2023 (KB5002453) - Microsoft Support						
5029568	高危	August 8, 2023- Security Only Update for .NET Framework 3.5, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Windows Server 2012 R2 (KB5029568) - Microsoft Support	CVE-2023-36899	Elevation of Privilege	Important	No	No	2
			CVE-2023-36873	Spoofing	Important	No	No	2
5002328	高危	Description of the security update for Project 2016: August 8, 2023 (KB5002328) -	ADV230003	Defense in Depth	Moderate	Yes	Yes	0

		Microsoft Support						
5028952	高危	August 8, 2023-KB5028952 Cumulative Update for .NET Framework 4.8 for Windows 10, version 1607 and Windows Server 2016 - Microsoft Support	CVE-2023-36899	Elevation of Privilege	Important	No	No	2
			CVE-2023-36873	Spoofing	Important	No	No	2
5029648	高危	August 8, 2023-KB5029648 Cumulative Update for .NET Framework 3.5, 4.8 and 4.8.1 for Windows 10 Version 21H2 - Microsoft Support	CVE-2023-36899	Elevation of Privilege	Important	No	No	2
			CVE-2023-36873	Spoofing	Important	No	No	2
5029569	高危	August 8, 2023-Security Only Update for .NET	CVE-2023-36899	Elevation of Privilege	Important	No	No	2
			CVE-2023-36873	Spoofing	Important	No	No	2

		Framework 2.0, 3.0, 4.6.2 for Windows Server 2008 SP2 (KB5029569) - Microsoft Support						
4504720	高危	Description of the security update for PowerPoint 2016: August 8, 2023 (KB4504720) - Microsoft Support	ADV230003	Defense in Depth	Moderate	Yes	Yes	0
5029652	高危	August 8, 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 Server 2012 (KB5029652) -	CVE-2023-36899	Elevation of Privilege	Important	No	No	2
			CVE-2023-36873	Spoofing	Important	No	No	2

		Microsoft Support						
5028948	高危	August 8, 2023-KB5028948 Cumulative Update for .NET Framework 3.5 and 4.8.1 for Windows 11, version 22H2 - Microsoft Support	CVE-2023-36899	Elevation of Privilege	Important	No	No	2
			CVE-2023-36873	Spoofing	Important	No	No	2
5029567	高危	August 8, 2023-Security Only Update for .NET Framework 3.5, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Windows Server 2012 (KB5029567) - Microsoft Support	CVE-2023-36899	Elevation of Privilege	Important	No	No	2
			CVE-2023-36873	Spoofing	Important	No	No	2
5002391	高危	Description of the security update for	ADV230003	Defense in Depth	Moderate	Yes	Yes	0

		Publisher 2013: August 8, 2023 (KB5002391) - Microsoft Support						
5002418	高危	Description of the security update for Visio 2016: August 8, 2023 (KB5002418) - Microsoft Support	ADV230003	Defense in Depth	Moderate	Yes	Yes	0
5029653	高危	August 8, 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 Server 2012 R2 (KB5029653) - Microsoft Support	CVE-2023-36899	Elevation of Privilege	Important	No	No	2
			CVE-2023-36873	Spoofing	Important	No	No	2

5002463	高危	Description of the security update for Excel 2016: August 8, 2023 (KB5002463) - Microsoft Support	CVE-2023-36896	Remote Code Execution	Important	No	No	2
			ADV230003	Defense in Depth	Moderate	Yes	Yes	0
5029566	高危	August 8, 2023- Security Only 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 (KB5029566) - Microsoft Support	CVE-2023-36899	Elevation of Privilege	Important	No	No	2
			CVE-2023-36873	Spoofing	Important	No	No	2
5029654	高危	August 8, 2023- Security and	CVE-2023-36899	Elevation of Privilege	Important	No	No	2
			CVE-2023-36873	Spoofing	Important	No	No	2

		Quality Rollup for .NET Framework 2.0, 3.0, 4.6.2 for Windows Server 2008 SP2 (KB5029654) - Microsoft Support						
5029651	高危	August 8, 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 (KB5029651) - Microsoft Support	CVE-2023-36899	Elevation of Privilege	Important	No	No	2
			CVE-2023-36873	Spoofing	Important	No	No	2
5029655	高危	August 8, 2023-	CVE-2023-36899	Elevation of Privilege	Important	No	No	2

		KB5029655 Cumulative Update for .NET Framework 3.5, 4.8 and 4.8.1 for Windows Server 2022 - Microsoft Support	CVE-2023-36873	Spoofing	Important	No	No	2
5029649	高危	August 8, 2023- KB5029649 Cumulative Update for .NET Framework 3.5, 4.8 and 4.8.1 for Windows 10 Version 22H2 - Microsoft Support	CVE-2023-36899	Elevation of Privilege	Important	No	No	2
			CVE-2023-36873	Spoofing	Important	No	No	2
4484489	高危	Description of the security update for Project 2013: August 8, 2023 (KB4484489) - Microsoft Support	ADV230003	Defense in Depth	Moderate	Yes	Yes	0

5002462	高危	Description of the security update for Publisher 2016: August 8, 2023 (KB5002462) - Microsoft Support	ADV230003	Defense in Depth	Moderate	Yes	Yes	0

本月发布内容无一般性更新补丁。

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