奇安信集团 2023 年 5 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 5 月 10 日

目　录

文档信息

文档名称	奇安信集团 2023 年 5 月补丁库更新通告		
文档编号	Qi An Xin Group-MSPatch-2023-0501		
发布日期	2023-05-10	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:2023.05.10.1,V10版本:2023.05.10.1000)已发布，本次更新推送了21个微软安全补丁，修复了29个安全漏洞，其中6个微软官方评级为“严重(Critical)”，23个评级为“重要(Important)”，这些漏洞影响Windows、Internet Explorer、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
5026370	CVE-2023-29324	Security Feature Bypass	Important	No	No	Exploitation More Likely
5026372						
5026426						
5026413						
5026409						
5026362						
5026382						
5026411						
5026366						
5026368						
5026415						
5026427						
5026361						
5026408						
5026363						
5026419						
5026370	CVE-2023-24943	Remote Code Execution	Critical	No	No	Exploitation Less Likely
5026372						
5026426						
5026413						
5026409						
5026362						
5026382						
5026411						
5026368						
5026415						
5026427						
5026361						

5026408 5026363 5026419						
5026370 5026409 5026362 5026411 5026415 5026363 5026419	CVE-2023-24941	Remote Code Execution	Critical	No	No	Exploitation More Likely
5026370 5026372 5026426 5026413 5026409 5026362 5026382 5026411 5026368 5026415 5026427 5026361 5026408 5026363 5026419	CVE-2023-29325	Remote Code Execution	Critical	Yes	No	Exploitation More Likely
5026370 5026372 5026426 5026413 5026409 5026362 5026382 5026411 5026368 5026415 5026427 5026361 5026408 5026363 5026419	CVE-2023-24932	Security Feature Bypass	Important	Yes	Yes	Exploitation Detected
5026370	CVE-2023-24903		Critical	No	No	

5026372 5026426 5026413 5026409 5026362 5026382 5026411 5026368 5026415 5026427 5026361 5026408 5026363 5026419		Remote Code Execution				Exploitation Less Likely
5026370 5026372 5026426 5026413 5026409 5026362 5026382 5026411 5026368 5026415 5026427 5026361 5026408 5026363 5026419	CVE-2023-28283	Remote Code Execution	Critical	No	No	Exploitation Less Likely
5026370 5026372 5026362 5026368 5026361	CVE-2023-24949	Elevation of Privilege	Important	No	No	Exploitation More Likely
5026372 5026368	CVE-2023-24902	Elevation of Privilege	Important	No	No	Exploitation More Likely
5026426 5026413 5026409 5026382 5026411	CVE-2023-29336	Elevation of Privilege	Important	No	Yes	Exploitation Detected

5026415						
5026427						
5026408						
5026363						
5026419						
5002397	CVE-2023-24954	Information Disclosure	Important	No	No	Exploitation More Likely
5002397	CVE-2023-24950	Spoofing	Important	No	No	Exploitation More Likely
5002397	CVE-2023-24955	Remote Code Execution	Critical	No	No	Exploitation More Likely

第3章 已知问题和特殊调整

本月暂无已知问题和特殊调整。

第4章 漏洞补丁详细列表

本月微软发布的系统安全更新补丁共 15 个，详细列表如下：

KBID	奇安信集团级别	补丁名称	CVE 编号	漏洞的影响	漏洞等级	公开披露	已受攻击	漏洞的可利用性
5026370	高危	May 9, 2023—KB5026370 (OS Build 20348.1726) - Microsoft Support for Windows Server 2022	CVE-2023-24945	Information Disclosure	Important	No	No	2
			CVE-2023-29324	Security Feature Bypass	Important	No	No	1
			CVE-2023-24940	Denial of Service	Important	No	No	2
			CVE-2023-24943	Remote Code Execution	Critical	No	No	2
			CVE-2023-24941	Remote Code Execution	Critical	No	No	1
			CVE-2023-24942	Denial of Service	Important	No	No	2
			CVE-2023-24939	Denial of Service	Important	No	No	2
			CVE-2023-29325	Remote Code Execution	Critical	Yes	No	1
			CVE-2023-28251	Security Feature Bypass	Important	No	No	2
			CVE-2023-24932	Security Feature Bypass	Important	Yes	Yes	0
			CVE-2023-24900	Information Disclosure	Important	No	No	2
			CVE-2023-24944	Information Disclosure	Important	No	No	2
			CVE-2023-24899	Elevation of Privilege	Important	No	No	2

			CVE-2023-24903	Remote Code Execution	Critical	No	No	2
			CVE-2023-28283	Remote Code Execution	Critical	No	No	2
			CVE-2023-24901	Information Disclosure	Important	No	No	2
			CVE-2023-24949	Elevation of Privilege	Important	No	No	1
5026372	高危	May 9, 2023—KB5026372 (OS Build 22621.1702) - Microsoft Support for Windows 11 version 22H2, all editions	CVE-2023-24943	Remote Code Execution	Critical	No	No	2
			CVE-2023-24905	Remote Code Execution	Important	No	No	2
			CVE-2023-24932	Security Feature Bypass	Important	Yes	Yes	0
			CVE-2023-28283	Remote Code Execution	Critical	No	No	2
			CVE-2023-24949	Elevation of Privilege	Important	No	No	1
			CVE-2023-24945	Information Disclosure	Important	No	No	2
			CVE-2023-24939	Denial of Service	Important	No	No	2
			CVE-2023-28251	Security Feature Bypass	Important	No	No	2
			CVE-2023-24903	Remote Code Execution	Critical	No	No	2
			CVE-2023-24901	Information Disclosure	Important	No	No	2
			CVE-2023-24940	Denial of Service	Important	No	No	2
			CVE-2023-24946	Elevation of Privilege	Important	No	No	2
			CVE-2023-24942	Denial of Service	Important	No	No	2
			CVE-2023-24900	Information Disclosure	Important	No	No	2
			CVE-2023-24944	Information Disclosure	Important	No	No	2

			CVE-2023-29324	Security Feature Bypass	Important	No	No	1
			CVE-2023-24902	Elevation of Privilege	Important	No	No	1
			CVE-2023-29325	Remote Code Execution	Critical	Yes	No	1
			CVE-2023-24899	Elevation of Privilege	Important	No	No	2
5026426	高危	May 9, 2023—KB5026426 (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-2023-24945	Information Disclosure	Important	No	No	2
			CVE-2023-29324	Security Feature Bypass	Important	No	No	1
			CVE-2023-24940	Denial of Service	Important	No	No	2
			CVE-2023-24946	Elevation of Privilege	Important	No	No	2
			CVE-2023-24943	Remote Code Execution	Critical	No	No	2
			CVE-2023-24942	Denial of Service	Important	No	No	2
			CVE-2023-29325	Remote Code Execution	Critical	Yes	No	1
			CVE-2023-28251	Security Feature Bypass	Important	No	No	2
			CVE-2023-24932	Security Feature Bypass	Important	Yes	Yes	0
			CVE-2023-24900	Information Disclosure	Important	No	No	2
			CVE-2023-24903	Remote Code Execution	Critical	No	No	2
			CVE-2023-28283	Remote Code Execution	Critical	No	No	2
			CVE-2023-24904	Elevation of Privilege	Important	No	No	2
			CVE-2023-29336	Elevation of Privilege	Important	No	Yes	0
5026413	高危	May 9, 2023—	CVE-2023-24945	Information Disclosure	Important	No	No	2

		KB5026413 (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-2023-29324	Security Feature Bypass	Important	No	No	1
			CVE-2023-24940	Denial of Service	Important	No	No	2
			CVE-2023-24946	Elevation of Privilege	Important	No	No	2
			CVE-2023-24943	Remote Code Execution	Critical	No	No	2
			CVE-2023-24942	Denial of Service	Important	No	No	2
			CVE-2023-29325	Remote Code Execution	Critical	Yes	No	1
			CVE-2023-28251	Security Feature Bypass	Important	No	No	2
			CVE-2023-24932	Security Feature Bypass	Important	Yes	Yes	0
			CVE-2023-24900	Information Disclosure	Important	No	No	2
			CVE-2023-24903	Remote Code Execution	Critical	No	No	2
			CVE-2023-28283	Remote Code Execution	Critical	No	No	2
			CVE-2023-24904	Elevation of Privilege	Important	No	No	2
			CVE-2023-29336	Elevation of Privilege	Important	No	Yes	0
5026409	高危	May 9, 2023—KB5026409 (Security-only update) - Microsoft Support for Windows Server 2012 R2,Windows	CVE-2023-24945	Information Disclosure	Important	No	No	2
			CVE-2023-29324	Security Feature Bypass	Important	No	No	1
			CVE-2023-24940	Denial of Service	Important	No	No	2
			CVE-2023-24943	Remote Code Execution	Critical	No	No	2
			CVE-2023-24941	Remote Code Execution	Critical	No	No	1
			CVE-2023-24948	Elevation of Privilege	Important	No	No	2

		Embedded 8.1 Industry Enterprise,Windows Embedded 8.1 Industry Pro	CVE-2023-24942	Denial of Service	Important	No	No	2
			CVE-2023-24939	Denial of Service	Important	No	No	2
			CVE-2023-29325	Remote Code Execution	Critical	Yes	No	1
			CVE-2023-28251	Security Feature Bypass	Important	No	No	2
			CVE-2023-24932	Security Feature Bypass	Important	Yes	Yes	0
			CVE-2023-24900	Information Disclosure	Important	No	No	2
			CVE-2023-24903	Remote Code Execution	Critical	No	No	2
			CVE-2023-28283	Remote Code Execution	Critical	No	No	2
			CVE-2023-24901	Information Disclosure	Important	No	No	2
			CVE-2023-29336	Elevation of Privilege	Important	No	Yes	0
5026362	高危	May 9, 2023—KB5026362 (OS Build 17763.4377) - Microsoft Support for Win 10 Ent LTSC v2019,Win 10 IoT Ent LTSC v2019,Windows 10 IoT Core 2019 LTSC,Windows Server 2019	CVE-2023-24943	Remote Code Execution	Critical	No	No	2
			CVE-2023-24932	Security Feature Bypass	Important	Yes	Yes	0
			CVE-2023-24947	Remote Code Execution	Important	No	No	2
			CVE-2023-28283	Remote Code Execution	Critical	No	No	2
			CVE-2023-24949	Elevation of Privilege	Important	No	No	1
			CVE-2023-24945	Information Disclosure	Important	No	No	2
			CVE-2023-24939	Denial of Service	Important	No	No	2
			CVE-2023-28251	Security Feature Bypass	Important	No	No	2
			CVE-2023-24903	Remote Code Execution	Critical	No	No	2

			CVE-2023-24901	Information Disclosure	Important	No	No	2
			CVE-2023-24940	Denial of Service	Important	No	No	2
			CVE-2023-24946	Elevation of Privilege	Important	No	No	2
			CVE-2023-24941	Remote Code Execution	Critical	No	No	1
			CVE-2023-24942	Denial of Service	Important	No	No	2
			CVE-2023-24900	Information Disclosure	Important	No	No	2
			CVE-2023-24944	Information Disclosure	Important	No	No	2
			CVE-2023-29324	Security Feature Bypass	Important	No	No	1
			CVE-2023-24948	Elevation of Privilege	Important	No	No	2
			CVE-2023-29325	Remote Code Execution	Critical	Yes	No	1
5026382	高危	May 9, 2023—KB5026382 (OS Build 10240.19926) - Microsoft Support for Windows 10	CVE-2023-24945	Information Disclosure	Important	No	No	2
			CVE-2023-29324	Security Feature Bypass	Important	No	No	1
			CVE-2023-24940	Denial of Service	Important	No	No	2
			CVE-2023-24946	Elevation of Privilege	Important	No	No	2
			CVE-2023-24943	Remote Code Execution	Critical	No	No	2
			CVE-2023-24948	Elevation of Privilege	Important	No	No	2
			CVE-2023-24942	Denial of Service	Important	No	No	2
			CVE-2023-24939	Denial of Service	Important	No	No	2
			CVE-2023-29325	Remote Code Execution	Critical	Yes	No	1

			CVE-2023-28251	Security Feature Bypass	Important	No	No	2
			CVE-2023-24932	Security Feature Bypass	Important	Yes	Yes	0
			CVE-2023-24900	Information Disclosure	Important	No	No	2
			CVE-2023-24903	Remote Code Execution	Critical	No	No	2
			CVE-2023-28283	Remote Code Execution	Critical	No	No	2
			CVE-2023-24901	Information Disclosure	Important	No	No	2
			CVE-2023-29336	Elevation of Privilege	Important	No	Yes	0
5026411	高危	May 9, 2023—KB5026411 (Security-only update) - Microsoft Support for Windows Server 2012,Windows Embedded 8 Standard	CVE-2023-24945	Information Disclosure	Important	No	No	2
			CVE-2023-29324	Security Feature Bypass	Important	No	No	1
			CVE-2023-24940	Denial of Service	Important	No	No	2
			CVE-2023-24943	Remote Code Execution	Critical	No	No	2
			CVE-2023-24941	Remote Code Execution	Critical	No	No	1
			CVE-2023-24948	Elevation of Privilege	Important	No	No	2
			CVE-2023-24942	Denial of Service	Important	No	No	2
			CVE-2023-24939	Denial of Service	Important	No	No	2
			CVE-2023-29325	Remote Code Execution	Critical	Yes	No	1
			CVE-2023-28251	Security Feature Bypass	Important	No	No	2
			CVE-2023-24932	Security Feature Bypass	Important	Yes	Yes	0

			CVE-2023-24900	Information Disclosure	Important	No	No	2
			CVE-2023-24903	Remote Code Execution	Critical	No	No	2
			CVE-2023-28283	Remote Code Execution	Critical	No	No	2
			CVE-2023-24901	Information Disclosure	Important	No	No	2
			CVE-2023-29336	Elevation of Privilege	Important	No	Yes	0
5026368	高危	May 9, 2023—KB5026368 (OS Build 22000.1936) - Microsoft Support for Windows 11 version 21H2, all editions	CVE-2023-24943	Remote Code Execution	Critical	No	No	2
			CVE-2023-24905	Remote Code Execution	Important	No	No	2
			CVE-2023-24932	Security Feature Bypass	Important	Yes	Yes	0
			CVE-2023-28283	Remote Code Execution	Critical	No	No	2
			CVE-2023-24949	Elevation of Privilege	Important	No	No	1
			CVE-2023-24945	Information Disclosure	Important	No	No	2
			CVE-2023-24939	Denial of Service	Important	No	No	2
			CVE-2023-28251	Security Feature Bypass	Important	No	No	2
			CVE-2023-24903	Remote Code Execution	Critical	No	No	2
			CVE-2023-24901	Information Disclosure	Important	No	No	2
			CVE-2023-24940	Denial of Service	Important	No	No	2
			CVE-2023-24946	Elevation of Privilege	Important	No	No	2
			CVE-2023-24942	Denial of Service	Important	No	No	2
			CVE-2023-24900	Information Disclosure	Important	No	No	2

			CVE-2023-24944	Information Disclosure	Important	No	No	2
			CVE-2023-29324	Security Feature Bypass	Important	No	No	1
			CVE-2023-24902	Elevation of Privilege	Important	No	No	1
			CVE-2023-24948	Elevation of Privilege	Important	No	No	2
			CVE-2023-29325	Remote Code Execution	Critical	Yes	No	1
			CVE-2023-24899	Elevation of Privilege	Important	No	No	2
5026415	高危	May 9, 2023—KB5026415 (Monthly Rollup) - Microsoft Support for Windows Server 2012 R2,Windows Embedded 8.1 Industry Enterprise,Windows Embedded 8.1 Industry Pro	CVE-2023-24945	Information Disclosure	Important	No	No	2
			CVE-2023-29324	Security Feature Bypass	Important	No	No	1
			CVE-2023-24940	Denial of Service	Important	No	No	2
			CVE-2023-24943	Remote Code Execution	Critical	No	No	2
			CVE-2023-24941	Remote Code Execution	Critical	No	No	1
			CVE-2023-24948	Elevation of Privilege	Important	No	No	2
			CVE-2023-24942	Denial of Service	Important	No	No	2
			CVE-2023-24939	Denial of Service	Important	No	No	2
			CVE-2023-29325	Remote Code Execution	Critical	Yes	No	1
			CVE-2023-28251	Security Feature Bypass	Important	No	No	2
			CVE-2023-24932	Security Feature Bypass	Important	Yes	Yes	0
			CVE-2023-24900	Information Disclosure	Important	No	No	2
			CVE-2023-24903	Remote Code Execution	Critical	No	No	2

			CVE-2023-28283	Remote Code Execution	Critical	No	No	2
			CVE-2023-24901	Information Disclosure	Important	No	No	2
			CVE-2023-29336	Elevation of Privilege	Important	No	Yes	0
5026427	高危	May 9, 2023—KB5026427 (Security-only update) - Microsoft Support for Windows Server 2008 Datacenter ESU,Windows Server 2008 Standard ESU,Windows Server 2008 Enterprise ESU	CVE-2023-24945	Information Disclosure	Important	No	No	2
			CVE-2023-29324	Security Feature Bypass	Important	No	No	1
			CVE-2023-24940	Denial of Service	Important	No	No	2
			CVE-2023-24943	Remote Code Execution	Critical	No	No	2
			CVE-2023-24942	Denial of Service	Important	No	No	2
			CVE-2023-29325	Remote Code Execution	Critical	Yes	No	1
			CVE-2023-28251	Security Feature Bypass	Important	No	No	2
			CVE-2023-24932	Security Feature Bypass	Important	Yes	Yes	0
			CVE-2023-24900	Information Disclosure	Important	No	No	2
			CVE-2023-24903	Remote Code Execution	Critical	No	No	2
			CVE-2023-28283	Remote Code Execution	Critical	No	No	2
			CVE-2023-24904	Elevation of Privilege	Important	No	No	2
			CVE-2023-29336	Elevation of Privilege	Important	No	Yes	0
5026361	高危	May 9, 2023—KB5026361 (OS Builds 19042.2965, 19044.2965	CVE-2023-24943	Remote Code Execution	Critical	No	No	2
			CVE-2023-24905	Remote Code Execution	Important	No	No	2
			CVE-2023-24932	Security Feature Bypass	Important	Yes	Yes	0

		, and 19045.2965) - Microsoft Support for Windows 10 Enterprise Multi-Session, version 20H2,Windows 10 Enterprise and Education, version 20H2,Windows 10 IoT Enterprise, version 20H2,Windows 10 on Surface Hub,Windows 10, version 21H2, all editions,Windows 10, version 22H2, all editions	CVE-2023-24947	Remote Code Execution	Important	No	No	2
			CVE-2023-28283	Remote Code Execution	Critical	No	No	2
			CVE-2023-24949	Elevation of Privilege	Important	No	No	1
			CVE-2023-24945	Information Disclosure	Important	No	No	2
			CVE-2023-24939	Denial of Service	Important	No	No	2
			CVE-2023-28251	Security Feature Bypass	Important	No	No	2
			CVE-2023-24903	Remote Code Execution	Critical	No	No	2
			CVE-2023-24901	Information Disclosure	Important	No	No	2
			CVE-2023-24940	Denial of Service	Important	No	No	2
			CVE-2023-24946	Elevation of Privilege	Important	No	No	2
			CVE-2023-24942	Denial of Service	Important	No	No	2
			CVE-2023-24900	Information Disclosure	Important	No	No	2
			CVE-2023-24944	Information Disclosure	Important	No	No	2
			CVE-2023-29324	Security Feature Bypass	Important	No	No	1
			CVE-2023-24948	Elevation of Privilege	Important	No	No	2
			CVE-2023-29325	Remote Code Execution	Critical	Yes	No	1
5026408	高危	May 9, 2023—KB5026408 (Monthly Rollup) - Microsoft Support	CVE-2023-24945	Information Disclosure	Important	No	No	2
			CVE-2023-29324	Security Feature Bypass	Important	No	No	1
			CVE-2023-24940	Denial of Service	Important	No	No	2

		for Windows Server 2008 Datacenter ESU,Windows Server 2008 Standard ESU,Windows Server 2008 Enterprise ESU	CVE-2023-24943	Remote Code Execution	Critical	No	No	2
			CVE-2023-24942	Denial of Service	Important	No	No	2
			CVE-2023-29325	Remote Code Execution	Critical	Yes	No	1
			CVE-2023-28251	Security Feature Bypass	Important	No	No	2
			CVE-2023-24932	Security Feature Bypass	Important	Yes	Yes	0
			CVE-2023-24900	Information Disclosure	Important	No	No	2
			CVE-2023-24903	Remote Code Execution	Critical	No	No	2
			CVE-2023-28283	Remote Code Execution	Critical	No	No	2
			CVE-2023-24904	Elevation of Privilege	Important	No	No	2
			CVE-2023-29336	Elevation of Privilege	Important	No	Yes	0
5026363	高危	May 9, 2023—KB5026363 (OS Build 14393.5921) - Microsoft Support for Windows 10, version 1607, all editions,Windows Server 2016, all editions	CVE-2023-24945	Information Disclosure	Important	No	No	2
			CVE-2023-29324	Security Feature Bypass	Important	No	No	1
			CVE-2023-24940	Denial of Service	Important	No	No	2
			CVE-2023-24946	Elevation of Privilege	Important	No	No	2
			CVE-2023-24943	Remote Code Execution	Critical	No	No	2
			CVE-2023-24941	Remote Code Execution	Critical	No	No	1
			CVE-2023-24948	Elevation of Privilege	Important	No	No	2
			CVE-2023-24942	Denial of Service	Important	No	No	2
			CVE-2023-24939	Denial of Service	Important	No	No	2

			CVE-2023-29325	Remote Code Execution	Critical	Yes	No	1
			CVE-2023-28251	Security Feature Bypass	Important	No	No	2
			CVE-2023-24932	Security Feature Bypass	Important	Yes	Yes	0
			CVE-2023-24900	Information Disclosure	Important	No	No	2
			CVE-2023-24947	Remote Code Execution	Important	No	No	2
			CVE-2023-24903	Remote Code Execution	Critical	No	No	2
			CVE-2023-28283	Remote Code Execution	Critical	No	No	2
			CVE-2023-24901	Information Disclosure	Important	No	No	2
			CVE-2023-29336	Elevation of Privilege	Important	No	Yes	0
5026419	高危	May 9, 2023—KB5026419 (Monthly Rollup) - Microsoft Support for Windows Server 2012,Windows Embedded 8 Standard	CVE-2023-24945	Information Disclosure	Important	No	No	2
			CVE-2023-29324	Security Feature Bypass	Important	No	No	1
			CVE-2023-24940	Denial of Service	Important	No	No	2
			CVE-2023-24943	Remote Code Execution	Critical	No	No	2
			CVE-2023-24941	Remote Code Execution	Critical	No	No	1
			CVE-2023-24948	Elevation of Privilege	Important	No	No	2
			CVE-2023-24942	Denial of Service	Important	No	No	2
			CVE-2023-24939	Denial of Service	Important	No	No	2
			CVE-2023-29325	Remote Code Execution	Critical	Yes	No	1
			CVE-2023-28251	Security Feature Bypass	Important	No	No	2

			CVE-2023-24932	Security Feature Bypass	Important	Yes	Yes	0
			CVE-2023-24900	Information Disclosure	Important	No	No	2
			CVE-2023-24903	Remote Code Execution	Critical	No	No	2
			CVE-2023-28283	Remote Code Execution	Critical	No	No	2
			CVE-2023-24901	Information Disclosure	Important	No	No	2
			CVE-2023-29336	Elevation of Privilege	Important	No	Yes	0

本月微软发布的软件安全更新补丁共 6 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
5002384	高危	Description of the security update for Excel 2013: May 9, 2023 (KB5002384) - Microsoft Support	CVE-2023-24953	Remote Code Execution	Important	No	No	2
5002386	高危	Description of the security update for Excel 2016: May 9, 2023 (KB5002386) - Microsoft Support	CVE-2023-24953	Remote Code Execution	Important	No	No	2
5002369	高危	Description of the security update for	CVE-2023-29335	Security Feature Bypass	Important	No	No	2

		Word 2016: May 9, 2023 (KB5002369) - Microsoft Support						
5026366	高危	KB5026366: Cumulative security update for Internet Explorer: May 9, 2023 - Microsoft Support	CVE-2023-29324	Security Feature Bypass	Important	No	No	1
5002397	高危	Description of the security update for SharePoint Enterprise Server 2016: May 9, 2023 (KB5002397) - Microsoft Support	CVE-2023-24954	Information Disclosure	Important	No	No	1
			CVE-2023-24950	Spoofing	Important	No	No	1
			CVE-2023-24955	Remote Code Execution	Critical	No	No	1
5002365	高危	Description of the security update for Word 2013: May 9, 2023 (KB5002365) - Microsoft Support	CVE-2023-29335	Security Feature Bypass	Important	No	No	2

本月发布内容 2 个一般性更新补丁。

KBID	奇安信集团级别	详细信息
4504725	其他功能性补丁	Office 2013 更新程序
5002297	其他功能性补丁	Office 2013 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