奇安信集团 2023 年 11 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 11 月 15 日

目 录

第 1 章 安全通告 2

第 2 章 重点关注补丁 3

第 3 章 已知问题和特殊调整 6

第 4 章 漏洞补丁详细列表 7

第 5 章 参考链接 37

文档信息

文档名称	奇安信集团 2023 年 11 月补丁库更新通告		
文档编号	Qi An Xin Group-MSPatch-2023-1101		
发布日期	2023-11-15	密级	公开
关键字	Microsoft、漏洞、补丁		
发布团队	奇安信集团漏洞补丁运营团队		

第1章 安全通告

尊敬的客户：

奇安信集团最新补丁库(V6版本:2023.11.15.1,V10版本:2023.11.15.1000)已发布，本次更新推送了32个微软安全补丁，修复了44个安全漏洞，其中2个微软官方评级为“严重(Critical)”，42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 17 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
5002517	CVE-2023-38177	Remote Code Execution	Important	No	No	Exploitation More Likely
5032254	CVE-2023-36036	Elevation of Privilege	Important	No	Yes	Exploitation Detected
5032190						
5032197						
5032189						
5032247						
5032248						
5032249						
5032196						
5032252						
5032250						
5032192						
5032199						
5032198						
5032254	CVE-2023-36397	Remote Code Execution	Critical	No	No	Exploitation Less Likely
5032190						
5032197						
5032189						
5032247						
5032248						
5032249						
5032196						
5032252						
5032250						
5032192						
5032199						
5032198						

5032254 5032190 5032197 5032189 5032247 5032248 5032249 5032196 5032252 5032250 5032192 5032199 5032198	CVE-2023-36424	Elevation of Privilege	Important	No	No	Exploitation More Likely
5032254 5032190 5032197 5032189 5032247 5032248 5032249 5032196 5032252 5032250 5032192 5032199 5032198	CVE-2023-36025	Security Feature Bypass	Important	No	Yes	Exploitation Detected
5032190 5032189 5032196 5032192 5032198	CVE-2023-38545	Remote Code Execution	Important	Yes	No	
5032190 5032197 5032189 5032196 5032192 5032199 5032198	CVE-2023-36400	Elevation of Privilege	Critical	No	No	Exploitation Less Likely
5032190 5032189 5032196	CVE-2023-38039	Denial of Service	Low	Yes	No	

5032192 5032198						
5032190 5032189 5032196 5032192 5032198	CVE-2023-36033	Elevation of Privilege	Important	Yes	Yes	Exploitation Detected
5032190 5032192 5032198	CVE-2023-36399	Elevation of Privilege	Important	No	No	Exploitation More Likely
5032190 5032197 5032189 5032191 5032247 5032249 5032196 5032252 5032250 5032192 5032199 5032198	CVE-2023-36017	Remote Code Execution	Important	No	No	Exploitation More Likely
5032197 5032189 5032196 5032192 5032199 5032198	CVE-2023-36394	Elevation of Privilege	Important	No	No	Exploitation More Likely
5002521	CVE-2023-36413	Security Feature Bypass	Important	Yes	No	Exploitation More Likely
5032146 5032147	CVE-2023-36035	Spoofing	Important	No	No	Exploitation More Likely
5032146 5032147	CVE-2023-36439	Remote Code Execution	Important	No	No	Exploitation More Likely
5032146 5032147	CVE-2023-36050	Spoofing	Important	No	No	Exploitation More Likely
5032146 5032147	CVE-2023-36039	Spoofing	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 13 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
5032254	高危	November 14, 2023—KB5032254 (Monthly Rollup) - Microsoft Support for Windows Server 2008 Datacenter ESU,Windows Server 2008 Standard ESU,Windows Server 2008 Enterprise ESU	CVE-2023-36705	Elevation of Privilege	Important	No	No	2
			CVE-2023-36425	Remote Code Execution	Important	No	No	2
			CVE-2023-36036	Elevation of Privilege	Important	No	Yes	0
			CVE-2023-36403	Elevation of Privilege	Important	No	No	2
			CVE-2023-36393	Remote Code Execution	Important	No	No	2
			CVE-2023-36397	Remote Code Execution	Critical	No	No	2
			CVE-2023-36424	Elevation of Privilege	Important	No	No	1
			CVE-2023-36402	Remote Code Execution	Important	No	No	2
			CVE-2023-36025	Security Feature Bypass	Important	No	Yes	0
			CVE-2023-36395	Denial of Service	Important	No	No	2

			CVE-2023-36428	Information Disclosure	Important	No	No	2
			CVE-2023-36719	Elevation of Privilege	Important	No	No	2
			CVE-2023-36423	Remote Code Execution	Important	No	No	2
			CVE-2023-36401	Remote Code Execution	Important	No	No	2
5032190	高危	November 14, 2023—KB5032190 (OS Builds 22621.2715 and 22631.2715) - Microsoft Support for Windows 11 version 22H2, all editions,Windows 11 version 23H2, all editions	CVE-2023-36036	Elevation of Privilege	Important	No	Yes	0
			CVE-2023-36028	Remote Code Execution	Important	No	No	2
			CVE-2023-36407	Elevation of Privilege	Important	No	No	2
			CVE-2023-24023	Spoofing	Important	No	No	2
			CVE-2023-36025	Security Feature Bypass	Important	No	Yes	0
			CVE-2023-36719	Elevation of Privilege	Important	No	No	2
			CVE-2023-36406	Information Disclosure	Important	No	No	2
			CVE-2023-36405	Elevation of Privilege	Important	No	No	2
			CVE-2023-36401	Remote Code Execution	Important	No	No	2
			CVE-2023-38545	Remote Code Execution	Important	Yes	No	4

			CVE-2023-36047	Elevation of Privilege	Important	No	No	2
			CVE-2023-36403	Elevation of Privilege	Important	No	No	2
			CVE-2023-36393	Remote Code Execution	Important	No	No	2
			CVE-2023-36397	Remote Code Execution	Critical	No	No	2
			CVE-2023-36408	Elevation of Privilege	Important	No	No	2
			CVE-2023-36425	Remote Code Execution	Important	No	No	2
			CVE-2023-36404	Information Disclosure	Important	No	No	2
			CVE-2023-36400	Elevation of Privilege	Critical	No	No	2
			CVE-2023-38039	Denial of Service	Low	Yes	No	4
			CVE-2023-36033	Elevation of Privilege	Important	Yes	Yes	0
			CVE-2023-36398	Information Disclosure	Important	No	No	2
			CVE-2023-36428	Information Disclosure	Important	No	No	2
			CVE-2023-36046	Denial of Service	Important	No	No	2

			CVE-2023-36705	Elevation of Privilege	Important	No	No	2
			CVE-2023-36399	Elevation of Privilege	Important	No	No	1
			CVE-2023-36427	Elevation of Privilege	Important	No	No	2
			CVE-2023-36017	Remote Code Execution	Important	No	No	1
			CVE-2023-36424	Elevation of Privilege	Important	No	No	1
			CVE-2023-36396	Remote Code Execution	Important	No	No	2
			CVE-2023-36402	Remote Code Execution	Important	No	No	2
			CVE-2023-36423	Remote Code Execution	Important	No	No	2
5032197	高危	November 14, 2023—KB5032197 (OS Build 14393.6452) - Microsoft Support for Windows 10, version 1607, all editions,Windows Server	CVE-2023-36036	Elevation of Privilege	Important	No	Yes	0
			CVE-2023-36028	Remote Code Execution	Important	No	No	2
			CVE-2023-36025	Security Feature Bypass	Important	No	Yes	0
			CVE-2023-36395	Denial of Service	Important	No	No	2
			CVE-2023-36719	Elevation of Privilege	Important	No	No	2
			CVE-2023-36405	Elevation of Privilege	Important	No	No	2

		2016, all editions	CVE-2023-36401	Remote Code Execution	Important	No	No	2
			CVE-2023-36403	Elevation of Privilege	Important	No	No	2
			CVE-2023-36393	Remote Code Execution	Important	No	No	2
			CVE-2023-36392	Denial of Service	Important	No	No	2
			CVE-2023-36397	Remote Code Execution	Critical	No	No	2
			CVE-2023-36408	Elevation of Privilege	Important	No	No	2
			CVE-2023-36425	Remote Code Execution	Important	No	No	2
			CVE-2023-36049	Elevation of Privilege	Important	No	No	2
			CVE-2023-36404	Information Disclosure	Important	No	No	2
			CVE-2023-36394	Elevation of Privilege	Important	No	No	1
			CVE-2023-36400	Elevation of Privilege	Critical	No	No	2
			CVE-2023-36398	Information Disclosure	Important	No	No	2
			CVE-2023-36428	Information Disclosure	Important	No	No	2

			CVE-2023-36560	Security Feature Bypass	Important	No	No	2
			CVE-2023-36705	Elevation of Privilege	Important	No	No	2
			CVE-2023-36017	Remote Code Execution	Important	No	No	1
			CVE-2023-36424	Elevation of Privilege	Important	No	No	1
			CVE-2023-36402	Remote Code Execution	Important	No	No	2
			CVE-2023-36423	Remote Code Execution	Important	No	No	2
5032189	高危	November 14, 2023—KB5032189 (OS Builds 19044.3693 and 19045.3693) - Microsoft Support for Windows 10 Enterprise and Education, version 21H2,Windows 10 IoT Enterprise, version 21H2,Windows 10	CVE-2023-36036	Elevation of Privilege	Important	No	Yes	0
			CVE-2023-36028	Remote Code Execution	Important	No	No	2
			CVE-2023-24023	Spoofing	Important	No	No	2
			CVE-2023-36025	Security Feature Bypass	Important	No	Yes	0
			CVE-2023-36719	Elevation of Privilege	Important	No	No	2
			CVE-2023-36405	Elevation of Privilege	Important	No	No	2
			CVE-2023-36401	Remote Code Execution	Important	No	No	2
			CVE-2023-38545	Remote Code Execution	Important	Yes	No	4

		Enterprise Multi-Session, version 21H2,Windows 10, version 22H2, all editions	CVE-2023-36047	Elevation of Privilege	Important	No	No	2
			CVE-2023-36403	Elevation of Privilege	Important	No	No	2
			CVE-2023-36393	Remote Code Execution	Important	No	No	2
			CVE-2023-36397	Remote Code Execution	Critical	No	No	2
			CVE-2023-36408	Elevation of Privilege	Important	No	No	2
			CVE-2023-36425	Remote Code Execution	Important	No	No	2
			CVE-2023-36404	Information Disclosure	Important	No	No	2
			CVE-2023-36394	Elevation of Privilege	Important	No	No	1
			CVE-2023-36400	Elevation of Privilege	Critical	No	No	2
			CVE-2023-38039	Denial of Service	Low	Yes	No	4
			CVE-2023-36033	Elevation of Privilege	Important	Yes	Yes	0
			CVE-2023-36398	Information Disclosure	Important	No	No	2
			CVE-2023-36428	Information Disclosure	Important	No	No	2

			CVE-2023-36705	Elevation of Privilege	Important	No	No	2
			CVE-2023-36427	Elevation of Privilege	Important	No	No	2
			CVE-2023-36017	Remote Code Execution	Important	No	No	1
			CVE-2023-36424	Elevation of Privilege	Important	No	No	1
			CVE-2023-36402	Remote Code Execution	Important	No	No	2
			CVE-2023-36423	Remote Code Execution	Important	No	No	2
5032247	高危	November 14, 2023—KB5032247 (Monthly Rollup) - Microsoft Support for Windows Server 2012	CVE-2023-36705	Elevation of Privilege	Important	No	No	2
			CVE-2023-36425	Remote Code Execution	Important	No	No	2
			CVE-2023-36036	Elevation of Privilege	Important	No	Yes	0
			CVE-2023-36403	Elevation of Privilege	Important	No	No	2
			CVE-2023-36393	Remote Code Execution	Important	No	No	2
			CVE-2023-36392	Denial of Service	Important	No	No	2
			CVE-2023-36397	Remote Code Execution	Critical	No	No	2
			CVE-2023-36017	Remote Code Execution	Important	No	No	1

			CVE-2023-36424	Elevation of Privilege	Important	No	No	1
			CVE-2023-36398	Information Disclosure	Important	No	No	2
			CVE-2023-36402	Remote Code Execution	Important	No	No	2
			CVE-2023-36025	Security Feature Bypass	Important	No	Yes	0
			CVE-2023-36395	Denial of Service	Important	No	No	2
			CVE-2023-36428	Information Disclosure	Important	No	No	2
			CVE-2023-36719	Elevation of Privilege	Important	No	No	2
			CVE-2023-36423	Remote Code Execution	Important	No	No	2
			CVE-2023-36401	Remote Code Execution	Important	No	No	2
5032248	高危	November 14, 2023—KB5032248 (Security-only update) - Microsoft Support for Windows Server 2008	CVE-2023-36705	Elevation of Privilege	Important	No	No	2
			CVE-2023-36425	Remote Code Execution	Important	No	No	2
			CVE-2023-36036	Elevation of Privilege	Important	No	Yes	0
			CVE-2023-36403	Elevation of Privilege	Important	No	No	2

		Datacenter ESU,Windows Server 2008 Standard ESU,Windows Server 2008 Enterprise ESU	CVE-2023-36393	Remote Code Execution	Important	No	No	2
			CVE-2023-36397	Remote Code Execution	Critical	No	No	2
			CVE-2023-36424	Elevation of Privilege	Important	No	No	1
			CVE-2023-36402	Remote Code Execution	Important	No	No	2
			CVE-2023-36025	Security Feature Bypass	Important	No	Yes	0
			CVE-2023-36395	Denial of Service	Important	No	No	2
			CVE-2023-36428	Information Disclosure	Important	No	No	2
			CVE-2023-36719	Elevation of Privilege	Important	No	No	2
			CVE-2023-36423	Remote Code Execution	Important	No	No	2
			CVE-2023-36401	Remote Code Execution	Important	No	No	2
5032249	高危	November 14, 2023—KB5032249 (Monthly Rollup) - Microsoft Support for Windows Server 2012 R2	CVE-2023-36705	Elevation of Privilege	Important	No	No	2
			CVE-2023-36425	Remote Code Execution	Important	No	No	2
			CVE-2023-36036	Elevation of Privilege	Important	No	Yes	0
			CVE-2023-36403	Elevation of Privilege	Important	No	No	2

			CVE-2023-36393	Remote Code Execution	Important	No	No	2
			CVE-2023-36392	Denial of Service	Important	No	No	2
			CVE-2023-36397	Remote Code Execution	Critical	No	No	2
			CVE-2023-36017	Remote Code Execution	Important	No	No	1
			CVE-2023-36424	Elevation of Privilege	Important	No	No	1
			CVE-2023-36398	Information Disclosure	Important	No	No	2
			CVE-2023-36402	Remote Code Execution	Important	No	No	2
			CVE-2023-36025	Security Feature Bypass	Important	No	Yes	0
			CVE-2023-36395	Denial of Service	Important	No	No	2
			CVE-2023-36428	Information Disclosure	Important	No	No	2
			CVE-2023-36719	Elevation of Privilege	Important	No	No	2
			CVE-2023-36423	Remote Code Execution	Important	No	No	2
			CVE-2023-36401	Remote Code Execution	Important	No	No	2
5032196	高危	November 14, 2023—KB5032196	CVE-2023-36036	Elevation of Privilege	Important	No	Yes	0

		(OS Build 17763.5122) - Microsoft Support for Win 10 Ent LTSC 2019,Win 10 IoT Ent LTSC 2019,Windows 10 IoT Core 2019 LTSC,Windows Server 2019	CVE-2023-36028	Remote Code Execution	Important	No	No	2
			CVE-2023-24023	Spoofing	Important	No	No	2
			CVE-2023-36025	Security Feature Bypass	Important	No	Yes	0
			CVE-2023-36395	Denial of Service	Important	No	No	2
			CVE-2023-36719	Elevation of Privilege	Important	No	No	2
			CVE-2023-36405	Elevation of Privilege	Important	No	No	2
			CVE-2023-36401	Remote Code Execution	Important	No	No	2
			CVE-2023-38545	Remote Code Execution	Important	Yes	No	4
			CVE-2023-36047	Elevation of Privilege	Important	No	No	2
			CVE-2023-36403	Elevation of Privilege	Important	No	No	2
			CVE-2023-36393	Remote Code Execution	Important	No	No	2
			CVE-2023-36392	Denial of Service	Important	No	No	2
			CVE-2023-36397	Remote Code Execution	Critical	No	No	2
			CVE-2023-36408	Elevation of Privilege	Important	No	No	2
			CVE-2023-36425	Remote Code Execution	Important	No	No	2

			CVE-2023-36404	Information Disclosure	Important	No	No	2
			CVE-2023-36394	Elevation of Privilege	Important	No	No	1
			CVE-2023-36400	Elevation of Privilege	Critical	No	No	2
			CVE-2023-38039	Denial of Service	Low	Yes	No	4
			CVE-2023-36033	Elevation of Privilege	Important	Yes	Yes	0
			CVE-2023-36398	Information Disclosure	Important	No	No	2
			CVE-2023-36428	Information Disclosure	Important	No	No	2
			CVE-2023-36705	Elevation of Privilege	Important	No	No	2
			CVE-2023-36427	Elevation of Privilege	Important	No	No	2
			CVE-2023-36017	Remote Code Execution	Important	No	No	1
			CVE-2023-36424	Elevation of Privilege	Important	No	No	1
			CVE-2023-36402	Remote Code Execution	Important	No	No	2
			CVE-2023-36423	Remote Code Execution	Important	No	No	2

5032252	高危	November 14, 2023—KB5032252 (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 POSReady 7 ESU	CVE-2023-36705	Elevation of Privilege	Important	No	No	2
			CVE-2023-36425	Remote Code Execution	Important	No	No	2
			CVE-2023-36036	Elevation of Privilege	Important	No	Yes	0
			CVE-2023-36403	Elevation of Privilege	Important	No	No	2
			CVE-2023-36393	Remote Code Execution	Important	No	No	2
			CVE-2023-36397	Remote Code Execution	Critical	No	No	2
			CVE-2023-36017	Remote Code Execution	Important	No	No	1
			CVE-2023-36424	Elevation of Privilege	Important	No	No	1
			CVE-2023-36402	Remote Code Execution	Important	No	No	2
			CVE-2023-36025	Security Feature Bypass	Important	No	Yes	0
			CVE-2023-36395	Denial of Service	Important	No	No	2
			CVE-2023-36428	Information Disclosure	Important	No	No	2
			CVE-2023-36719	Elevation of Privilege	Important	No	No	2
			CVE-2023-36423	Remote Code Execution	Important	No	No	2

			CVE-2023-36401	Remote Code Execution	Important	No	No	2
5032250	高危	November 14, 2023—KB5032250 (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 POSReady 7 ESU	CVE-2023-36705	Elevation of Privilege	Important	No	No	2
			CVE-2023-36425	Remote Code Execution	Important	No	No	2
			CVE-2023-36036	Elevation of Privilege	Important	No	Yes	0
			CVE-2023-36403	Elevation of Privilege	Important	No	No	2
			CVE-2023-36393	Remote Code Execution	Important	No	No	2
			CVE-2023-36397	Remote Code Execution	Critical	No	No	2
			CVE-2023-36017	Remote Code Execution	Important	No	No	1
			CVE-2023-36424	Elevation of Privilege	Important	No	No	1
			CVE-2023-36402	Remote Code Execution	Important	No	No	2
			CVE-2023-36025	Security Feature Bypass	Important	No	Yes	0
			CVE-2023-36395	Denial of Service	Important	No	No	2
			CVE-2023-36428	Information Disclosure	Important	No	No	2
			CVE-2023-36719	Elevation of Privilege	Important	No	No	2

			CVE-2023-36423	Remote Code Execution	Important	No	No	2
			CVE-2023-36401	Remote Code Execution	Important	No	No	2
5032192	高危	November 14, 2023—KB5032192 (OS Build 22000.2600) - Microsoft Support for Windows 11 version 21H2, all editions	CVE-2023-36036	Elevation of Privilege	Important	No	Yes	0
			CVE-2023-36028	Remote Code Execution	Important	No	No	2
			CVE-2023-36407	Elevation of Privilege	Important	No	No	2
			CVE-2023-24023	Spoofing	Important	No	No	2
			CVE-2023-36025	Security Feature Bypass	Important	No	Yes	0
			CVE-2023-36719	Elevation of Privilege	Important	No	No	2
			CVE-2023-36406	Information Disclosure	Important	No	No	2
			CVE-2023-36405	Elevation of Privilege	Important	No	No	2
			CVE-2023-36401	Remote Code Execution	Important	No	No	2
			CVE-2023-38545	Remote Code Execution	Important	Yes	No	4
			CVE-2023-36047	Elevation of Privilege	Important	No	No	2
			CVE-2023-36403	Elevation of Privilege	Important	No	No	2

			CVE-2023-36393	Remote Code Execution	Important	No	No	2
			CVE-2023-36397	Remote Code Execution	Critical	No	No	2
			CVE-2023-36408	Elevation of Privilege	Important	No	No	2
			CVE-2023-36425	Remote Code Execution	Important	No	No	2
			CVE-2023-36404	Information Disclosure	Important	No	No	2
			CVE-2023-36394	Elevation of Privilege	Important	No	No	1
			CVE-2023-36400	Elevation of Privilege	Critical	No	No	2
			CVE-2023-38039	Denial of Service	Low	Yes	No	4
			CVE-2023-36033	Elevation of Privilege	Important	Yes	Yes	0
			CVE-2023-36398	Information Disclosure	Important	No	No	2
			CVE-2023-36428	Information Disclosure	Important	No	No	2
			CVE-2023-36046	Denial of Service	Important	No	No	2
			CVE-2023-36705	Elevation of Privilege	Important	No	No	2

			CVE-2023-36399	Elevation of Privilege	Important	No	No	1
			CVE-2023-36427	Elevation of Privilege	Important	No	No	2
			CVE-2023-36017	Remote Code Execution	Important	No	No	1
			CVE-2023-36424	Elevation of Privilege	Important	No	No	1
			CVE-2023-36402	Remote Code Execution	Important	No	No	2
			CVE-2023-36423	Remote Code Execution	Important	No	No	2
5032199	高危	November 14, 2023—KB5032199 (OS Build 10240.20308) - Microsoft Support for Windows 10	CVE-2023-36036	Elevation of Privilege	Important	No	Yes	0
			CVE-2023-36028	Remote Code Execution	Important	No	No	2
			CVE-2023-36025	Security Feature Bypass	Important	No	Yes	0
			CVE-2023-36719	Elevation of Privilege	Important	No	No	2
			CVE-2023-36401	Remote Code Execution	Important	No	No	2
			CVE-2023-36403	Elevation of Privilege	Important	No	No	2
			CVE-2023-36393	Remote Code Execution	Important	No	No	2
			CVE-2023-36397	Remote Code Execution	Critical	No	No	2

			CVE-2023-36425	Remote Code Execution	Important	No	No	2
			CVE-2023-36049	Elevation of Privilege	Important	No	No	2
			CVE-2023-36394	Elevation of Privilege	Important	No	No	1
			CVE-2023-36400	Elevation of Privilege	Critical	No	No	2
			CVE-2023-36398	Information Disclosure	Important	No	No	2
			CVE-2023-36428	Information Disclosure	Important	No	No	2
			CVE-2023-36560	Security Feature Bypass	Important	No	No	2
			CVE-2023-36705	Elevation of Privilege	Important	No	No	2
			CVE-2023-36017	Remote Code Execution	Important	No	No	1
			CVE-2023-36424	Elevation of Privilege	Important	No	No	1
			CVE-2023-36402	Remote Code Execution	Important	No	No	2
			CVE-2023-36423	Remote Code Execution	Important	No	No	2
5032198	高危	November 14, 2023—KB5032198	CVE-2023-36036	Elevation of Privilege	Important	No	Yes	0

		(OS Build 20348.2113) - Microsoft Support for Windows Server 2022	CVE-2023-36028	Remote Code Execution	Important	No	No	2
			CVE-2023-36407	Elevation of Privilege	Important	No	No	2
			CVE-2023-24023	Spoofing	Important	No	No	2
			CVE-2023-36025	Security Feature Bypass	Important	No	Yes	0
			CVE-2023-36395	Denial of Service	Important	No	No	2
			CVE-2023-36719	Elevation of Privilege	Important	No	No	2
			CVE-2023-36406	Information Disclosure	Important	No	No	2
			CVE-2023-36405	Elevation of Privilege	Important	No	No	2
			CVE-2023-36401	Remote Code Execution	Important	No	No	2
			CVE-2023-38545	Remote Code Execution	Important	Yes	No	4
			CVE-2023-36047	Elevation of Privilege	Important	No	No	2
			CVE-2023-36403	Elevation of Privilege	Important	No	No	2
			CVE-2023-36393	Remote Code Execution	Important	No	No	2
			CVE-2023-36392	Denial of Service	Important	No	No	2
			CVE-2023-36397	Remote Code Execution	Critical	No	No	2

			CVE-2023-36408	Elevation of Privilege	Important	No	No	2
			CVE-2023-36425	Remote Code Execution	Important	No	No	2
			CVE-2023-36404	Information Disclosure	Important	No	No	2
			CVE-2023-36394	Elevation of Privilege	Important	No	No	1
			CVE-2023-36400	Elevation of Privilege	Critical	No	No	2
			CVE-2023-38039	Denial of Service	Low	Yes	No	4
			CVE-2023-36033	Elevation of Privilege	Important	Yes	Yes	0
			CVE-2023-36398	Information Disclosure	Important	No	No	2
			CVE-2023-36428	Information Disclosure	Important	No	No	2
			CVE-2023-36705	Elevation of Privilege	Important	No	No	2
			CVE-2023-36399	Elevation of Privilege	Important	No	No	1
			CVE-2023-36427	Elevation of Privilege	Important	No	No	2
			CVE-2023-36017	Remote Code Execution	Important	No	No	1

			CVE-2023-36424	Elevation of Privilege	Important	No	No	1
			CVE-2023-36402	Remote Code Execution	Important	No	No	2
			CVE-2023-36423	Remote Code Execution	Important	No	No	2

本月微软发布的软件安全更新补丁共 19 个，详细列表如下：

KBID	奇安信安全集团级别	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
5002517	高危	Description of the security update for SharePoint Enterprise Server 2016: November 14, 2023 (KB5002517) - Microsoft Support	CVE-2023-38177	Remote Code Execution	Important	No	No	1
5032191	高危	KB5032191: Cumulative security update for Internet Explorer: November 14, 2023 -	CVE-2023-36017	Remote Code Execution	Important	No	No	1

		Microsoft Support						
5032186	高危	November 14, 2023-Security Only Update for .NET Framework 2.0, 3.0, 4.6.2 for Windows Server 2008 SP2 (KB5032186) - Microsoft Support	CVE-2023-36560	Security Feature Bypass	Important	No	No	2
			CVE-2023-36049	Elevation of Privilege	Important	No	No	2
5002521	高危	Description of the security update for Office 2016: November 14, 2023 (KB5002521) - Microsoft Support	CVE-2023-36413	Security Feature Bypass	Important	Yes	No	1
5031989	高危	November 14, 2023-KB5031989 Cumulative Update for .NET Framework 4.8 for Windows 10, version 1607 and	CVE-2023-36560	Security Feature Bypass	Important	No	No	2
			CVE-2023-36049	Elevation of Privilege	Important	No	No	2

		Windows Server 2016 - Microsoft Support						
5002518	高危	Description of the security update for Excel 2016: November 14, 2023 (KB5002518) - Microsoft Support	CVE-2023-36041	Remote Code Execution	Important	No	No	2
			CVE-2023-36037	Security Feature Bypass	Important	No	No	2
5032336	高危	November 14, 2023-KB5032336 Cumulative Update for .NET Framework 3.5, 4.8 and 4.8.1 for Windows Server 2022 - Microsoft Support	CVE-2023-36560	Security Feature Bypass	Important	No	No	2
			CVE-2023-36049	Elevation of Privilege	Important	No	No	2
5032338	高危	November 14, 2023-KB5032338 Cumulative Update for .NET Framework 3.5, 4.8 and 4.8.1 for	CVE-2023-36560	Security Feature Bypass	Important	No	No	2
			CVE-2023-36049	Elevation of Privilege	Important	No	No	2

		Windows 10 Version 21H2 - Microsoft Support						
5032341	高危	November 14, 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 (KB5032341) - Microsoft Support	CVE-2023-36560	Security Feature Bypass	Important	No	No	2
			CVE-2023-36049	Elevation of Privilege	Important	No	No	2
5032185	高危	November 14, 2023-Security Only Update for .NET Framework 3.5.1, 4.6.2, 4.7, 4.7.1,	CVE-2023-36560	Security Feature Bypass	Important	No	No	2
			CVE-2023-36049	Elevation of Privilege	Important	No	No	2

		4.7.2, 4.8 for Windows Embedded 7 Standard and Windows Server 2008 R2 SP1 (KB5032185) - Microsoft Support						
5032146	高危	Description of the security update for Microsoft Exchange Server 2019 and 2016: November 14, 2023 (KB5032146) - Microsoft Support	CVE-2023-36035	Spoofing	Important	No	No	1
			CVE-2023-36439	Remote Code Execution	Important	No	No	1
			CVE-2023-36050	Spoofing	Important	No	No	1
			CVE-2023-36039	Spoofing	Important	No	No	1
5032344	高危	November 14, 2023-Security and Quality Rollup for .NET Framework 2.0, 3.0, 4.6.2 for Windows Server 2008 SP2	CVE-2023-36560	Security Feature Bypass	Important	No	No	2
			CVE-2023-36049	Elevation of Privilege	Important	No	No	2

		(KB5032344) - Microsoft Support						
5032007	高危	November 14, 2023-KB5032007 Cumulative Update for .NET Framework 3.5 and 4.8.1 for Windows 11, version 22H2 and Windows 11, version 23H2 - Microsoft Support	CVE-2023-36560	Security Feature Bypass	Important	No	No	2
			CVE-2023-36049	Elevation of Privilege	Important	No	No	2
5032147	高危	Description of the security update for Microsoft Exchange Server 2016: November 14, 2023 (KB5032147) - Microsoft Support	CVE-2023-36035	Spoofing	Important	No	No	1
			CVE-2023-36439	Remote Code Execution	Important	No	No	1
			CVE-2023-36050	Spoofing	Important	No	No	1
			CVE-2023-36039	Spoofing	Important	No	No	1
5032339	高危	November 14, 2023-KB5032339	CVE-2023-36560	Security Feature Bypass	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-2023-36049	Elevation of Privilege	Important	No	No	2
5032340	高危	November 14, 2023-KB5032340 Cumulative Update for .NET Framework 3.5, 4.8 and 4.8.1 for Windows 11, version 21H2 - Microsoft Support	CVE-2023-36560	Security Feature Bypass	Important	No	No	2
			CVE-2023-36049	Elevation of Privilege	Important	No	No	2
5032342	高危	November 14, 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-2023-36560	Security Feature Bypass	Important	No	No	2
			CVE-2023-36049	Elevation of Privilege	Important	No	No	2

		Windows Server 2012 (KB5032342) - Microsoft Support						
5032337	高危	November 14, 2023-KB5032337 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-2023-36560	Security Feature Bypass	Important	No	No	2
			CVE-2023-36049	Elevation of Privilege	Important	No	No	2
5032343	高危	November 14, 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	CVE-2023-36560	Security Feature Bypass	Important	No	No	2
			CVE-2023-36049	Elevation of Privilege	Important	No	No	2

		2012 R2 (KB5032343) - Microsoft Support						

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