奇安信集团 2023 年 9 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 9 月 13 日

目 录

文档信息

文档名称	奇安信集团 2023 年 9 月补丁库更新通告		
文档编号	Qi An Xin Group-MSPatch-2023-0901		
发布日期	2023-09-13	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:2023.09.13.1,V10版本:2023.09.13.1000)已发布，本次更新推送了37个微软安全补丁，修复了33个安全漏洞，其中4个微软官方评级为“严重(Critical)”，29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
5002497 5002483	CVE-2023-36761	Information Disclosure	Important	Yes	Yes	Exploitation Detected
5030217 5030271 5030211 5030220 5030216 5030286 5030214 5030269 5030261 5030213 5030279 5030287 5030265 5030278 5030219	CVE-2023-36804	Elevation of Privilege	Important	No	No	Exploitation More Likely
5030217 5030271 5030211 5030220 5030216 5030286 5030214 5030269 5030261 5030213 5030279	CVE-2023-38161	Elevation of Privilege	Important	No	No	Exploitation More Likely

5030287 5030265 5030278 5030219						
5030217 5030271 5030211 5030220 5030216 5030286 5030214 5030269 5030261 5030213 5030279 5030287 5030265 5030278 5030219	CVE-2023-38142	Elevation of Privilege	Important	No	No	Exploitation More Likely
5030217 5030271 5030211 5030220 5030216 5030286 5030214 5030269 5030261 5030213 5030279 5030287 5030265 5030278 5030219	CVE-2023-38144	Elevation of Privilege	Important	No	No	Exploitation More Likely
5030217 5030271 5030211 5030220 5030216 5030286 5030214	CVE-2023-38160	Information Disclosure	Important	No	No	Exploitation More Likely

5030269 5030261 5030213 5030279 5030287 5030265 5030278 5030219						
5030217 5030211 5030216 5030219	CVE-2023-38148	Remote Code Execution	Critical	No	No	Exploitation More Likely
5030217 5030211 5030216 5030214 5030219	CVE-2023-36802	Elevation of Privilege	Important	No	Yes	Exploitation Detected
5030217 5030271 5030211 5030220 5030216 5030286 5030214 5030269 5030261 5030213 5030279 5030287 5030265 5030278 5030219	CVE-2023-38143	Elevation of Privilege	Important	No	No	Exploitation More Likely
5030271 5030216 5030286 5030214 5030269 5030261 5030213 5030279 5030287	CVE-2023-38152	Information Disclosure	Important	No	No	Exploitation More Likely

5030265 5030278						
5030181 5029924 5030184 5030186 5030185 5030178 5030182 5030183 5030180 5030179	CVE-2023-36793	Remote Code Execution	Critical	No	No	Exploitation Less Likely
5030181 5029924 5030184 5030186 5030185 5030178 5030182 5030183 5030180 5030179	CVE-2023-36796	Remote Code Execution	Critical	No	No	Exploitation Less Likely
5030181 5029924 5030184 5030186 5030185 5030178 5030182 5030183 5030180 5030179	CVE-2023-36792	Remote Code Execution	Critical	No	No	Exploitation Less 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
5030217	高危	September 12, 2023—KB5030217 (OS Build 22000.2416) - Microsoft Support for Windows 11 version 21H2, all editions	CVE-2023-36804	Elevation of Privilege	Important	No	No	1
			CVE-2023-38140	Information Disclosure	Important	No	No	2
			CVE-2023-38150	Elevation of Privilege	Important	No	No	2
			CVE-2023-38146	Remote Code Execution	Important	No	No	2
			CVE-2023-38161	Elevation of Privilege	Important	No	No	1
			CVE-2023-38142	Elevation of Privilege	Important	No	No	1
			CVE-2023-38139	Elevation of Privilege	Important	No	No	2
			CVE-2023-38144	Elevation of Privilege	Important	No	No	1
			CVE-2023-38149	Denial of Service	Important	No	No	2
			CVE-2023-35355	Elevation of Privilege	Important	No	No	2
			CVE-2023-38147	Remote Code Execution	Important	No	No	2
			CVE-2023-38141	Elevation of Privilege	Important	No	No	2
			CVE-2023-38160	Information Disclosure	Important	No	No	1
			CVE-2023-38148	Remote Code Execution	Critical	No	No	1
			CVE-2023-36803	Information Disclosure	Important	No	No	2

			CVE-2023-36802	Elevation of Privilege	Important	No	Yes	0
			CVE-2023-38143	Elevation of Privilege	Important	No	No	1
			CVE-2023-36805	Security Feature Bypass	Important	No	No	2
5030271	高危	September 12, 2023—KB5030271 (Monthly Rollup) - Microsoft Support for Windows Server 2008 Datacenter ESU,Windows Server 2008 Standard ESU,Windows Server 2008 Enterprise ESU	CVE-2023-36804	Elevation of Privilege	Important	No	No	1
			CVE-2023-38161	Elevation of Privilege	Important	No	No	1
			CVE-2023-38142	Elevation of Privilege	Important	No	No	1
			CVE-2023-38139	Elevation of Privilege	Important	No	No	2
			CVE-2023-38144	Elevation of Privilege	Important	No	No	1
			CVE-2023-38141	Elevation of Privilege	Important	No	No	2
			CVE-2023-38160	Information Disclosure	Important	No	No	1
			CVE-2023-36801	Information Disclosure	Important	No	No	2
			CVE-2023-38152	Information Disclosure	Important	No	No	1
			CVE-2023-38143	Elevation of Privilege	Important	No	No	1
5030211	高危	September 12, 2023—KB5030211 (OS Builds 19044.3448 and 19045.3448) - Microsoft Support	CVE-2023-36804	Elevation of Privilege	Important	No	No	1
			CVE-2023-38140	Information Disclosure	Important	No	No	2
			CVE-2023-38161	Elevation of Privilege	Important	No	No	1
			CVE-2023-38142	Elevation of Privilege	Important	No	No	1
			CVE-2023-38139	Elevation of Privilege	Important	No	No	2
			CVE-2023-38144	Elevation of Privilege	Important	No	No	1

		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-2023-38149	Denial of Service	Important	No	No	2
			CVE-2023-35355	Elevation of Privilege	Important	No	No	2
			CVE-2023-38147	Remote Code Execution	Important	No	No	2
			CVE-2023-38141	Elevation of Privilege	Important	No	No	2
			CVE-2023-38160	Information Disclosure	Important	No	No	1
			CVE-2023-38148	Remote Code Execution	Critical	No	No	1
			CVE-2023-36803	Information Disclosure	Important	No	No	2
			CVE-2023-36802	Elevation of Privilege	Important	No	Yes	0
			CVE-2023-38143	Elevation of Privilege	Important	No	No	1
			CVE-2023-36805	Security Feature Bypass	Important	No	No	2
5030220	高危	September 12, 2023—KB5030220 (OS Build 10240.20162) - Microsoft Support for Windows 10	CVE-2023-36804	Elevation of Privilege	Important	No	No	1
			CVE-2023-38161	Elevation of Privilege	Important	No	No	1
			CVE-2023-38142	Elevation of Privilege	Important	No	No	1
			CVE-2023-38139	Elevation of Privilege	Important	No	No	2
			CVE-2023-38144	Elevation of Privilege	Important	No	No	1
			CVE-2023-38149	Denial of Service	Important	No	No	2
			CVE-2023-38147	Remote Code Execution	Important	No	No	2
			CVE-2023-38141	Elevation of Privilege	Important	No	No	2
			CVE-2023-38160	Information Disclosure	Important	No	No	1

			CVE-2023-38143	Elevation of Privilege	Important	No	No	1
			CVE-2023-36805	Security Feature Bypass	Important	No	No	2
5030216	高危	September 12, 2023—KB5030216 (OS Build 20348.1970) - Microsoft Support for Windows Server 2022	CVE-2023-38161	Elevation of Privilege	Important	No	No	1
			CVE-2023-38142	Elevation of Privilege	Important	No	No	1
			CVE-2023-38149	Denial of Service	Important	No	No	2
			CVE-2023-38144	Elevation of Privilege	Important	No	No	1
			CVE-2023-38147	Remote Code Execution	Important	No	No	2
			CVE-2023-38160	Information Disclosure	Important	No	No	1
			CVE-2023-38148	Remote Code Execution	Critical	No	No	1
			CVE-2023-38140	Information Disclosure	Important	No	No	2
			CVE-2023-35355	Elevation of Privilege	Important	No	No	2
			CVE-2023-36801	Information Disclosure	Important	No	No	2
			CVE-2023-36803	Information Disclosure	Important	No	No	2
			CVE-2023-38162	Denial of Service	Important	No	No	2
			CVE-2023-38139	Elevation of Privilege	Important	No	No	2
			CVE-2023-38141	Elevation of Privilege	Important	No	No	2
			CVE-2023-38152	Information Disclosure	Important	No	No	1
			CVE-2023-36805	Security Feature Bypass	Important	No	No	2
			CVE-2023-36804	Elevation of Privilege	Important	No	No	1

			CVE-2023-36802	Elevation of Privilege	Important	No	Yes	0
			CVE-2023-38143	Elevation of Privilege	Important	No	No	1
5030286	高危	September 12, 2023—KB5030286 (Security-only update) - Microsoft Support for Windows Server 2008 Datacenter ESU,Windows Server 2008 Standard ESU,Windows Server 2008 Enterprise ESU	CVE-2023-36804	Elevation of Privilege	Important	No	No	1
			CVE-2023-38161	Elevation of Privilege	Important	No	No	1
			CVE-2023-38142	Elevation of Privilege	Important	No	No	1
			CVE-2023-38139	Elevation of Privilege	Important	No	No	2
			CVE-2023-38144	Elevation of Privilege	Important	No	No	1
			CVE-2023-38141	Elevation of Privilege	Important	No	No	2
			CVE-2023-38160	Information Disclosure	Important	No	No	1
			CVE-2023-36801	Information Disclosure	Important	No	No	2
			CVE-2023-38152	Information Disclosure	Important	No	No	1
			CVE-2023-38143	Elevation of Privilege	Important	No	No	1
5030214	高危	September 12, 2023—KB5030214 (OS Build 17763.4851) - Microsoft Support for Win 10 Ent LTSC v2019,Win 10 IoT	CVE-2023-36804	Elevation of Privilege	Important	No	No	1
			CVE-2023-38140	Information Disclosure	Important	No	No	2
			CVE-2023-38161	Elevation of Privilege	Important	No	No	1
			CVE-2023-38142	Elevation of Privilege	Important	No	No	1
			CVE-2023-38139	Elevation of Privilege	Important	No	No	2
			CVE-2023-38144	Elevation of Privilege	Important	No	No	1
			CVE-2023-38149	Denial of Service	Important	No	No	2

		Ent LTSC v2019,Windows 10 IoT Core 2019 LTSC,Windows Server 2019	CVE-2023-35355	Elevation of Privilege	Important	No	No	2
			CVE-2023-38147	Remote Code Execution	Important	No	No	2
			CVE-2023-38141	Elevation of Privilege	Important	No	No	2
			CVE-2023-38160	Information Disclosure	Important	No	No	1
			CVE-2023-36801	Information Disclosure	Important	No	No	2
			CVE-2023-38152	Information Disclosure	Important	No	No	1
			CVE-2023-36803	Information Disclosure	Important	No	No	2
			CVE-2023-36802	Elevation of Privilege	Important	No	Yes	0
			CVE-2023-38162	Denial of Service	Important	No	No	2
			CVE-2023-38143	Elevation of Privilege	Important	No	No	1
			CVE-2023-36805	Security Feature Bypass	Important	No	No	2
5030269	高危	September 12, 2023—KB5030269 (Monthly Rollup) - Microsoft Support for Windows Server 2012 R2	CVE-2023-36804	Elevation of Privilege	Important	No	No	1
			CVE-2023-38161	Elevation of Privilege	Important	No	No	1
			CVE-2023-38142	Elevation of Privilege	Important	No	No	1
			CVE-2023-38139	Elevation of Privilege	Important	No	No	2
			CVE-2023-38144	Elevation of Privilege	Important	No	No	1
			CVE-2023-38149	Denial of Service	Important	No	No	2
			CVE-2023-38141	Elevation of Privilege	Important	No	No	2
			CVE-2023-38160	Information Disclosure	Important	No	No	1
			CVE-2023-36801	Information Disclosure	Important	No	No	2

			CVE-2023-38152	Information Disclosure	Important	No	No	1
			CVE-2023-38162	Denial of Service	Important	No	No	2
			CVE-2023-38143	Elevation of Privilege	Important	No	No	1
			CVE-2023-36805	Security Feature Bypass	Important	No	No	2
5030261	高危	September 12, 2023—KB5030261 (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	CVE-2023-36804	Elevation of Privilege	Important	No	No	1
			CVE-2023-38161	Elevation of Privilege	Important	No	No	1
			CVE-2023-38142	Elevation of Privilege	Important	No	No	1
			CVE-2023-38139	Elevation of Privilege	Important	No	No	2
			CVE-2023-38144	Elevation of Privilege	Important	No	No	1
			CVE-2023-38149	Denial of Service	Important	No	No	2
			CVE-2023-38141	Elevation of Privilege	Important	No	No	2
			CVE-2023-38160	Information Disclosure	Important	No	No	1
			CVE-2023-36801	Information Disclosure	Important	No	No	2
			CVE-2023-38152	Information Disclosure	Important	No	No	1
			CVE-2023-38143	Elevation of Privilege	Important	No	No	1

		POSReady 7 ESU						
5030213	高危	September 12, 2023—KB5030213 (OS Build 14393.6252) - Microsoft Support for Windows 10, version 1607, all editions, Windows Server 2016, all editions	CVE-2023-36804	Elevation of Privilege	Important	No	No	1
			CVE-2023-38140	Information Disclosure	Important	No	No	2
			CVE-2023-38161	Elevation of Privilege	Important	No	No	1
			CVE-2023-38142	Elevation of Privilege	Important	No	No	1
			CVE-2023-38139	Elevation of Privilege	Important	No	No	2
			CVE-2023-38144	Elevation of Privilege	Important	No	No	1
			CVE-2023-38149	Denial of Service	Important	No	No	2
			CVE-2023-38147	Remote Code Execution	Important	No	No	2
			CVE-2023-38141	Elevation of Privilege	Important	No	No	2
			CVE-2023-38160	Information Disclosure	Important	No	No	1
			CVE-2023-36801	Information Disclosure	Important	No	No	2
			CVE-2023-38152	Information Disclosure	Important	No	No	1
			CVE-2023-36803	Information Disclosure	Important	No	No	2
			CVE-2023-38162	Denial of Service	Important	No	No	2
			CVE-2023-38143	Elevation of Privilege	Important	No	No	1
			CVE-2023-36805	Security Feature Bypass	Important	No	No	2
5030279	高危	September 12, 2023—KB5030279 (Security-only	CVE-2023-36804	Elevation of Privilege	Important	No	No	1
			CVE-2023-38161	Elevation of Privilege	Important	No	No	1
			CVE-2023-38142	Elevation of Privilege	Important	No	No	1

		update) - Microsoft Support for Windows Server 2012	CVE-2023-38139	Elevation of Privilege	Important	No	No	2
			CVE-2023-38144	Elevation of Privilege	Important	No	No	1
			CVE-2023-38149	Denial of Service	Important	No	No	2
			CVE-2023-38141	Elevation of Privilege	Important	No	No	2
			CVE-2023-38160	Information Disclosure	Important	No	No	1
			CVE-2023-36801	Information Disclosure	Important	No	No	2
			CVE-2023-38152	Information Disclosure	Important	No	No	1
			CVE-2023-38162	Denial of Service	Important	No	No	2
			CVE-2023-38143	Elevation of Privilege	Important	No	No	1
5030287	高危	September 12, 2023—KB5030287 (Security-only update) - Microsoft Support for Windows Server 2012 R2	CVE-2023-36804	Elevation of Privilege	Important	No	No	1
			CVE-2023-38161	Elevation of Privilege	Important	No	No	1
			CVE-2023-38142	Elevation of Privilege	Important	No	No	1
			CVE-2023-38139	Elevation of Privilege	Important	No	No	2
			CVE-2023-38144	Elevation of Privilege	Important	No	No	1
			CVE-2023-38149	Denial of Service	Important	No	No	2
			CVE-2023-38141	Elevation of Privilege	Important	No	No	2
			CVE-2023-38160	Information Disclosure	Important	No	No	1
			CVE-2023-36801	Information Disclosure	Important	No	No	2
			CVE-2023-38152	Information Disclosure	Important	No	No	1
			CVE-2023-38162	Denial of Service	Important	No	No	2

			CVE-2023-38143	Elevation of Privilege	Important	No	No	1
			CVE-2023-36805	Security Feature Bypass	Important	No	No	2
5030265	高危	September 12, 2023—KB5030265 (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-2023-36804	Elevation of Privilege	Important	No	No	1
			CVE-2023-38161	Elevation of Privilege	Important	No	No	1
			CVE-2023-38142	Elevation of Privilege	Important	No	No	1
			CVE-2023-38139	Elevation of Privilege	Important	No	No	2
			CVE-2023-38144	Elevation of Privilege	Important	No	No	1
			CVE-2023-38149	Denial of Service	Important	No	No	2
			CVE-2023-38141	Elevation of Privilege	Important	No	No	2
			CVE-2023-38160	Information Disclosure	Important	No	No	1
			CVE-2023-36801	Information Disclosure	Important	No	No	2
			CVE-2023-38152	Information Disclosure	Important	No	No	1
			CVE-2023-38143	Elevation of Privilege	Important	No	No	1
5030278	高危	September 12, 2023—KB5030278	CVE-2023-36804	Elevation of Privilege	Important	No	No	1
			CVE-2023-38161	Elevation of Privilege	Important	No	No	1

		(Monthly Rollup) - Microsoft Support for Windows Server 2012	CVE-2023-38142	Elevation of Privilege	Important	No	No	1
			CVE-2023-38139	Elevation of Privilege	Important	No	No	2
			CVE-2023-38144	Elevation of Privilege	Important	No	No	1
			CVE-2023-38149	Denial of Service	Important	No	No	2
			CVE-2023-38141	Elevation of Privilege	Important	No	No	2
			CVE-2023-38160	Information Disclosure	Important	No	No	1
			CVE-2023-36801	Information Disclosure	Important	No	No	2
			CVE-2023-38152	Information Disclosure	Important	No	No	1
			CVE-2023-38162	Denial of Service	Important	No	No	2
			CVE-2023-38143	Elevation of Privilege	Important	No	No	1
5030219	高危	September 12, 2023—KB5030219 (OS Build 22621.2283) - Microsoft Support for Windows 11 version 22H2, all editions	CVE-2023-36804	Elevation of Privilege	Important	No	No	1
			CVE-2023-38150	Elevation of Privilege	Important	No	No	2
			CVE-2023-38146	Remote Code Execution	Important	No	No	2
			CVE-2023-38161	Elevation of Privilege	Important	No	No	1
			CVE-2023-38142	Elevation of Privilege	Important	No	No	1
			CVE-2023-38139	Elevation of Privilege	Important	No	No	2
			CVE-2023-38144	Elevation of Privilege	Important	No	No	1
			CVE-2023-38149	Denial of Service	Important	No	No	2
			CVE-2023-35355	Elevation of Privilege	Important	No	No	2
			CVE-2023-38147	Remote Code Execution	Important	No	No	2

			CVE-2023-38141	Elevation of Privilege	Important	No	No	2
			CVE-2023-38160	Information Disclosure	Important	No	No	1
			CVE-2023-38148	Remote Code Execution	Critical	No	No	1
			CVE-2023-36803	Information Disclosure	Important	No	No	2
			CVE-2023-36802	Elevation of Privilege	Important	No	Yes	0
			CVE-2023-38143	Elevation of Privilege	Important	No	No	1
			CVE-2023-36805	Security Feature Bypass	Important	No	No	2

本月微软发布的软件安全更新补丁共 22 个，详细列表如下：

KBID	奇安信集团级别	补丁名称	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
5002501	高危	Description of the security update for SharePoint Enterprise Server 2016 Language Pack: September	CVE-2023-36762	Remote Code Execution	Important	No	No	3

		12, 2023 (KB5002501) - Microsoft Support						
5002497	高危	Description of the security update for Word 2016: September 12, 2023 (KB5002497) - Microsoft Support	CVE-2023-36762	Remote Code Execution	Important	No	No	3
			CVE-2023-36761	Information Disclosure	Important	Yes	Yes	0
5002488	高危	Description of the security update for Excel 2013: September 12, 2023 (KB5002488) - Microsoft Support	CVE-2023-36766	Information Disclosure	Important	No	No	2
5002457	高危	Description of the security update for Office 2016: September 12, 2023 (KB5002457) - Microsoft Support	CVE-2023-41764	Spoofing	Moderate	No	No	2
			CVE-2023-36767	Security Feature Bypass	Important	No	No	2
5030181	高危	September 12, 2023-	CVE-2023-36793	Remote Code Execution	Critical	No	No	2

		KB5030181 Cumulative Update for .NET Framework 3.5, 4.8 and 4.8.1 for Windows 11, version 21H2 - Microsoft Support	CVE-2023-36796	Remote Code Execution	Critical	No	No	2
			CVE-2023-36792	Remote Code Execution	Critical	No	No	2
			CVE-2023-36794	Remote Code Execution	Important	No	No	2
			CVE-2023-36788	Remote Code Execution	Important	No	No	2
5029924	高危	September 12, 2023-KB5029924 Cumulative Update for .NET Framework 4.8 for Windows 10, version 1607 and Windows Server 2016 - Microsoft Support	CVE-2023-36796	Remote Code Execution	Critical	No	No	2
			CVE-2023-36792	Remote Code Execution	Critical	No	No	2
			CVE-2023-36793	Remote Code Execution	Critical	No	No	2
			CVE-2023-36794	Remote Code Execution	Important	No	No	2
5030184	高危	September 12, 2023-Security and Quality Rollup for .NET Framework 3.5, 4.6.2, 4.7,	CVE-2023-36793	Remote Code Execution	Critical	No	No	2
			CVE-2023-36796	Remote Code Execution	Critical	No	No	2
			CVE-2023-36792	Remote Code Execution	Critical	No	No	2
			CVE-2023-36794	Remote Code Execution	Important	No	No	2
			CVE-2023-36788	Remote Code Execution	Important	No	No	2

		4.7.1, 4.7.2, 4.8 for Windows Server 2012 R2 (KB5030184) - Microsoft Support						
5030186	高危	September 12, 2023-KB5030186 Cumulative Update for .NET Framework 3.5, 4.8 and 4.8.1 for Windows Server 2022 - Microsoft Support	CVE-2023-36793	Remote Code Execution	Critical	No	No	2
			CVE-2023-36796	Remote Code Execution	Critical	No	No	2
			CVE-2023-36792	Remote Code Execution	Critical	No	No	2
			CVE-2023-36794	Remote Code Execution	Important	No	No	2
			CVE-2023-36788	Remote Code Execution	Important	No	No	2
5030185	高危	September 12, 2023-Security and Quality Rollup for .NET Framework 2.0, 3.0, 4.6.2 for Windows Server 2008 SP2 (KB5030185) - Microsoft Support	CVE-2023-36793	Remote Code Execution	Critical	No	No	2
			CVE-2023-36796	Remote Code Execution	Critical	No	No	2
			CVE-2023-36792	Remote Code Execution	Critical	No	No	2
			CVE-2023-36794	Remote Code Execution	Important	No	No	2
			CVE-2023-36788	Remote Code Execution	Important	No	No	2

5030178	高危	September 12, 2023-KB5030178 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-2023-36793	Remote Code Execution	Critical	No	No	2
			CVE-2023-36796	Remote Code Execution	Critical	No	No	2
			CVE-2023-36792	Remote Code Execution	Critical	No	No	2
			CVE-2023-36794	Remote Code Execution	Important	No	No	2
			CVE-2023-36788	Remote Code Execution	Important	No	No	2
5002496	高危	Description of the security update for Excel 2016: September 12, 2023 (KB5002496) - Microsoft Support	CVE-2023-36766	Information Disclosure	Important	No	No	2
5002499	高危	Description of the security update for Outlook 2016: September 12, 2023 (KB5002499) -	CVE-2023-36763	Information Disclosure	Important	No	No	2

		Microsoft Support						
5030209	高危	KB5030209: Cumulative security update for Internet Explorer: September 12, 2023 - Microsoft Support	CVE-2023-36805	Security Feature Bypass	Important	No	No	2
5030182	高危	September 12, 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 (KB5030182) - Microsoft Support	CVE-2023-36793	Remote Code Execution	Critical	No	No	2
			CVE-2023-36796	Remote Code Execution	Critical	No	No	2
			CVE-2023-36792	Remote Code Execution	Critical	No	No	2
			CVE-2023-36794	Remote Code Execution	Important	No	No	2
			CVE-2023-36788	Remote Code Execution	Important	No	No	2
5002494	高危	Description of the security update for	CVE-2023-36762	Remote Code Execution	Important	No	No	3
			CVE-2023-36764	Elevation of Privilege	Important	No	No	2

		SharePoint Enterprise Server 2016: September 12, 2023 (KB5002494) - Microsoft Support						
5030183	高危	September 12, 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 (KB5030183) - Microsoft Support	CVE-2023-36793	Remote Code Execution	Critical	No	No	2
			CVE-2023-36796	Remote Code Execution	Critical	No	No	2
			CVE-2023-36792	Remote Code Execution	Critical	No	No	2
			CVE-2023-36794	Remote Code Execution	Important	No	No	2
			CVE-2023-36788	Remote Code Execution	Important	No	No	2
5002100	高危	Description of the security update for Office 2016: September 12, 2023 (KB5002100) -	CVE-2023-41764	Spoofing	Moderate	No	No	2

		Microsoft Support						
5030180	高危	September 12, 2023-KB5030180 Cumulative Update for .NET Framework 3.5, 4.8 and 4.8.1 for Windows 10 Version 22H2 - Microsoft Support	CVE-2023-36793	Remote Code Execution	Critical	No	No	2
			CVE-2023-36796	Remote Code Execution	Critical	No	No	2
			CVE-2023-36792	Remote Code Execution	Critical	No	No	2
			CVE-2023-36794	Remote Code Execution	Important	No	No	2
			CVE-2023-36788	Remote Code Execution	Important	No	No	2
5030179	高危	September 12, 2023-KB5030179 Cumulative Update for .NET Framework 3.5, 4.8 and 4.8.1 for Windows 10 Version 21H2 - Microsoft Support	CVE-2023-36793	Remote Code Execution	Critical	No	No	2
			CVE-2023-36796	Remote Code Execution	Critical	No	No	2
			CVE-2023-36792	Remote Code Execution	Critical	No	No	2
			CVE-2023-36794	Remote Code Execution	Important	No	No	2
			CVE-2023-36788	Remote Code Execution	Important	No	No	2
5002483	高危	Description of the security update for Word 2013: September 12, 2023 (KB5002483) -	CVE-2023-36761	Information Disclosure	Important	Yes	Yes	0

		Microsoft Support						
5002498	高危	Description of the security update for Office 2016: September 12, 2023 (KB5002498) - Microsoft Support	CVE-2023-41764	Spoofing	Moderate	No	No	2
5002477	高危	Description of the security update for Office 2013: September 12, 2023 (KB5002477) - Microsoft Support	CVE-2023-41764	Spoofing	Moderate	No	No	2
			CVE-2023-36767	Security Feature Bypass	Important	No	No	2

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