奇安信集团 2022 年 03 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

2022 年 03 月 09 日

目 录

文档信息

文档名称	奇安信集团 2022 年 03 月补丁库更新通告		
文档编号	Qi An Xin Group-MSPatch-2022-0301		
发布日期	2022-03-09	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:2022.03.09.1,V10版本:2022.03.09.1000)已发布，本次更新推送了 19 个微软安全补丁，修复了 36 个安全漏洞，其中 1 个微软官方评级为“严重(Critical)”，35 个评级为“重要(Important)”，这些漏洞影响产品 Windows、Internet Explorer、和 Microsoft Office。同时推送了 1 个非安全 Office 补丁。

2019 年 4 月 10 日发布的天擎 6.6.0.2000 及以上版本支持 Windows 10 安全更新补丁管理，如需此功能请更新版本。

第2章 重点关注补丁

本月有 11 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
5011503	CVE-2022-24459	Elevation of Privilege	Important	Yes	No	Exploitation Less Likely
5011495						
5011485						
5011527						
5011491						
5011535						
5011487						
5011534						
5011525						
5011493						
5011552						
5011560						
5011564						
5011529						
5011503	CVE-2022-24507	Elevation of Privilege	Important	No	No	Exploitation More Likely
5011495						
5011485						
5011487						
5011493						
5011503	CVE-2022-21990	Remote Code Execution	Important	Yes	No	Exploitation More Likely
5011495						
5011485						
5011527						
5011491						
5011535						
5011487						

5011534 5011525 5011493 5011552 5011560 5011564 5011529						
5011503 5011486 5011495 5011485 5011527 5011491 5011535 5011487 5011534 5011525 5011493 5011552 5011560 5011564 5011529	CVE-2022-23299	Elevation of Privilege	Important	No	No	Exploitation More Likely
5011503 5011485 5011487 5011493	CVE-2022-23286	Elevation of Privilege	Important	No	No	Exploitation More Likely
5011503 5011495 5011485 5011527 5011491 5011535 5011487 5011493 5011552 5011560 5011564 5011529	CVE-2022-23253	Denial of Service	Important	No	No	Exploitation More Likely
5011503 5011486 5011495	CVE-2022-24502	Security Feature Bypass	Important	No	No	Exploitation More Likely

5011485 5011527 5011491 5011535 5011487 5011534 5011525 5011493 5011552 5011560 5011564 5011529						
5011503 5011486 5011495 5011485 5011527 5011491 5011535 5011487 5011552 5011560 5011564 5011529	CVE-2022-23285	Remote Code Execution	Important	No	No	Exploitation More Likely
5011503 5011495 5011485 5011527 5011491 5011535 5011487 5011493 5011560 5011564	CVE-2022-23294	Remote Code Execution	Important	No	No	Exploitation More Likely
5012698 5010324	CVE-2022-23277	Remote Code Execution	Critical	No	No	Exploitation More Likely
5011487 5011493	CVE-2022-24508	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 14 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
5011503	高危	March 8, 2022—KB5011503 (OS Build 17763.2686) for Windows 10 Enterprise 2019 LTSC, Windows 10 IoT Enterprise 2019 LTSC, Windows 10 IoT Core 2019 LTSC	CVE-2022-24505	Elevation of Privilege	Important	No	No	2
			CVE-2022-24459	Elevation of Privilege	Important	Yes	No	2
			CVE-2022-24507	Elevation of Privilege	Important	No	No	1
			CVE-2022-21975	Denial of Service	Important	No	No	2
			CVE-2022-21967	Elevation of Privilege	Important	No	No	2
			CVE-2022-23288	Elevation of Privilege	Important	No	No	2
			CVE-2022-23284	Elevation of Privilege	Important	No	No	2
			CVE-2022-23293	Elevation of Privilege	Important	No	No	2
			CVE-2022-23298	Elevation of Privilege	Important	No	No	2
			CVE-2022-21990	Remote Code Execution	Important	Yes	No	1
			CVE-2022-23291	Elevation	Important	No	No	2

				of Privilege				
			CVE-2022-23299	Elevation of Privilege	Important	No	No	1
			CVE-2022-23286	Elevation of Privilege	Important	No	No	1
			CVE-2022-24460	Elevation of Privilege	Important	No	No	2
			CVE-2022-23283	Elevation of Privilege	Important	No	No	2
			CVE-2022-23281	Information Disclosure	Important	No	No	2
			CVE-2022-22010	Information Disclosure	Important	No	No	2
			CVE-2022-24455	Elevation of Privilege	Important	No	No	2
			CVE-2022-23287	Elevation of Privilege	Important	No	No	2
			CVE-2022-23297	Information Disclosure	Important	No	No	2
			CVE-2022-24503	Information Disclosure	Important	No	No	2
			CVE-2022-23253	Denial of Service	Important	No	No	1
			CVE-2022-23296	Elevation of Privilege	Important	No	No	2
			CVE-2022-24502	Security Feature Bypass	Important	No	No	1
			CVE-2022-23285	Remote Code Execution	Important	No	No	1
			CVE-2022-23294	Remote Code Execution	Important	No	No	1
			CVE-2022-21977	Information Disclosure	Important	No	No	2

			CVE-2022-23290	Elevation of Privilege	Important	No	No	2
			CVE-2022-24454	Elevation of Privilege	Important	No	No	2
			CVE-2022-23278	Spoofing	Important	No	No	2
5011495	高危	March 8, 2022—KB5011495 (OS Build 14393.5006) for Windows 10, version 1607, all editions ,Windows Server 2016, all editions	CVE-2022-24505	Elevation of Privilege	Important	No	No	2
			CVE-2022-24459	Elevation of Privilege	Important	Yes	No	2
			CVE-2022-24507	Elevation of Privilege	Important	No	No	1
			CVE-2022-21975	Denial of Service	Important	No	No	2
			CVE-2022-21967	Elevation of Privilege	Important	No	No	2
			CVE-2022-23284	Elevation of Privilege	Important	No	No	2
			CVE-2022-23293	Elevation of Privilege	Important	No	No	2
			CVE-2022-23298	Elevation of Privilege	Important	No	No	2
			CVE-2022-21990	Remote Code Execution	Important	Yes	No	1
			CVE-2022-23299	Elevation of Privilege	Important	No	No	1
			CVE-2022-24460	Elevation of Privilege	Important	No	No	2
			CVE-2022-23283	Elevation of Privilege	Important	No	No	2
			CVE-2022-23281	Information	Important	No	No	2

				Disclosure				
			CVE-2022-22010	Information Disclosure	Important	No	No	2
			CVE-2022-24455	Elevation of Privilege	Important	No	No	2
			CVE-2022-23287	Elevation of Privilege	Important	No	No	2
			CVE-2022-23297	Information Disclosure	Important	No	No	2
			CVE-2022-24503	Information Disclosure	Important	No	No	2
			CVE-2022-23253	Denial of Service	Important	No	No	1
			CVE-2022-23296	Elevation of Privilege	Important	No	No	2
			CVE-2022-24502	Security Feature Bypass	Important	No	No	1
			CVE-2022-23285	Remote Code Execution	Important	No	No	1
			CVE-2022-23294	Remote Code Execution	Important	No	No	1
			CVE-2022-21977	Information Disclosure	Important	No	No	2
			CVE-2022-23290	Elevation of Privilege	Important	No	No	2
			CVE-2022-24454	Elevation of Privilege	Important	No	No	2
5011485	高危	March 8, 2022—KB5011485 (OS Build 18363.2158) for Windows 10	CVE-2022-24505	Elevation of Privilege	Important	No	No	2
			CVE-2022-24507	Elevation of Privilege	Important	No	No	1
			CVE-2022-24459	Elevation of Privilege	Important	Yes	No	2

		Enterprise, version 1909,Windows 10 Enterprise and Education, version 1909,Windows 10 IoT Enterprise, version 1909	CVE-2022-21975	Denial of Service	Important	No	No	2
			CVE-2022-21967	Elevation of Privilege	Important	No	No	2
			CVE-2022-23288	Elevation of Privilege	Important	No	No	2
			CVE-2022-23284	Elevation of Privilege	Important	No	No	2
			CVE-2022-23293	Elevation of Privilege	Important	No	No	2
			CVE-2022-23298	Elevation of Privilege	Important	No	No	2
			CVE-2022-21990	Remote Code Execution	Important	Yes	No	1
			CVE-2022-23291	Elevation of Privilege	Important	No	No	2
			CVE-2022-23299	Elevation of Privilege	Important	No	No	1
			CVE-2022-23286	Elevation of Privilege	Important	No	No	1
			CVE-2022-24525	Elevation of Privilege	Important	No	No	2
			CVE-2022-24460	Elevation of Privilege	Important	No	No	2
			CVE-2022-23283	Elevation of Privilege	Important	No	No	2
			CVE-2022-23281	Information Disclosure	Important	No	No	2
			CVE-2022-22010	Information Disclosure	Important	No	No	2
			CVE-2022-24455	Elevation	Important	No	No	2

				of Privilege				
			CVE-2022-23287	Elevation of Privilege	Important	No	No	2
			CVE-2022-23297	Information Disclosure	Important	No	No	2
			CVE-2022-24503	Information Disclosure	Important	No	No	2
			CVE-2022-23253	Denial of Service	Important	No	No	1
			CVE-2022-23296	Elevation of Privilege	Important	No	No	2
			CVE-2022-24502	Security Feature Bypass	Important	No	No	1
			CVE-2022-23285	Remote Code Execution	Important	No	No	1
			CVE-2022-23294	Remote Code Execution	Important	No	No	1
			CVE-2022-21977	Information Disclosure	Important	No	No	2
			CVE-2022-23290	Elevation of Privilege	Important	No	No	2
			CVE-2022-24454	Elevation of Privilege	Important	No	No	2
			CVE-2022-23278	Spoofing	Important	No	No	2
5011527	高危	March 8, 2022—KB5011527 (Security-only update) for Windows Server 2012, Windows	CVE-2022-24459	Elevation of Privilege	Important	Yes	No	2
			CVE-2022-23284	Elevation of Privilege	Important	No	No	2
			CVE-2022-23293	Elevation of Privilege	Important	No	No	2
			CVE-2022-23298	Elevation of Privilege	Important	No	No	2

		Embedded 8 Standard	CVE-2022-21990	Remote Code Execution	Important	Yes	No	1
			CVE-2022-23299	Elevation of Privilege	Important	No	No	1
			CVE-2022-23283	Elevation of Privilege	Important	No	No	2
			CVE-2022-23281	Information Disclosure	Important	No	No	2
			CVE-2022-22010	Information Disclosure	Important	No	No	2
			CVE-2022-24455	Elevation of Privilege	Important	No	No	2
			CVE-2022-23297	Information Disclosure	Important	No	No	2
			CVE-2022-24503	Information Disclosure	Important	No	No	2
			CVE-2022-23253	Denial of Service	Important	No	No	1
			CVE-2022-23296	Elevation of Privilege	Important	No	No	2
			CVE-2022-24502	Security Feature Bypass	Important	No	No	1
			CVE-2022-23285	Remote Code Execution	Important	No	No	1
			CVE-2022-23294	Remote Code Execution	Important	No	No	1
			CVE-2022-23290	Elevation of Privilege	Important	No	No	2
			CVE-2022-21973	Denial of Service	Important	No	No	2
			CVE-2022-24454	Elevation of Privilege	Important	No	No	2
5011491	高危	March 8, 2022—KB501149	CVE-2022-24505	Elevation of Privilege	Important	No	No	2

		1 (OS Build 10240.19235) for Windows 10	CVE-2022-24459	Elevation of Privilege	Important	Yes	No	2
			CVE-2022-21975	Denial of Service	Important	No	No	2
			CVE-2022-21967	Elevation of Privilege	Important	No	No	2
			CVE-2022-23284	Elevation of Privilege	Important	No	No	2
			CVE-2022-23293	Elevation of Privilege	Important	No	No	2
			CVE-2022-23298	Elevation of Privilege	Important	No	No	2
			CVE-2022-21990	Remote Code Execution	Important	Yes	No	1
			CVE-2022-23299	Elevation of Privilege	Important	No	No	1
			CVE-2022-24460	Elevation of Privilege	Important	No	No	2
			CVE-2022-23283	Elevation of Privilege	Important	No	No	2
			CVE-2022-23281	Information Disclosure	Important	No	No	2
			CVE-2022-22010	Information Disclosure	Important	No	No	2
			CVE-2022-24455	Elevation of Privilege	Important	No	No	2
			CVE-2022-23287	Elevation of Privilege	Important	No	No	2
			CVE-2022-23297	Information Disclosure	Important	No	No	2
			CVE-2022-24503	Information Disclosure	Important	No	No	2

			CVE-2022-23253	Denial of Service	Important	No	No	1
			CVE-2022-23296	Elevation of Privilege	Important	No	No	2
			CVE-2022-24502	Security Feature Bypass	Important	No	No	1
			CVE-2022-23285	Remote Code Execution	Important	No	No	1
			CVE-2022-23294	Remote Code Execution	Important	No	No	1
			CVE-2022-21977	Information Disclosure	Important	No	No	2
			CVE-2022-23290	Elevation of Privilege	Important	No	No	2
			CVE-2022-24454	Elevation of Privilege	Important	No	No	2
5011535	可选的高危	March 8, 2022—KB5011535 (Monthly Rollup) for Windows Server 2012, Windows Embedded 8 Standard	CVE-2022-24459	Elevation of Privilege	Important	Yes	No	2
			CVE-2022-23284	Elevation of Privilege	Important	No	No	2
			CVE-2022-23293	Elevation of Privilege	Important	No	No	2
			CVE-2022-23298	Elevation of Privilege	Important	No	No	2
			CVE-2022-21990	Remote Code Execution	Important	Yes	No	1
			CVE-2022-23299	Elevation of Privilege	Important	No	No	1
			CVE-2022-23283	Elevation of Privilege	Important	No	No	2
			CVE-2022-23281	Information Disclosure	Important	No	No	2

			CVE-2022-22010	Information Disclosure	Important	No	No	2
			CVE-2022-24455	Elevation of Privilege	Important	No	No	2
			CVE-2022-23297	Information Disclosure	Important	No	No	2
			CVE-2022-24503	Information Disclosure	Important	No	No	2
			CVE-2022-23253	Denial of Service	Important	No	No	1
			CVE-2022-23296	Elevation of Privilege	Important	No	No	2
			CVE-2022-24502	Security Feature Bypass	Important	No	No	1
			CVE-2022-23285	Remote Code Execution	Important	No	No	1
			CVE-2022-23294	Remote Code Execution	Important	No	No	1
			CVE-2022-23290	Elevation of Privilege	Important	No	No	2
			CVE-2022-21973	Denial of Service	Important	No	No	2
			CVE-2022-24454	Elevation of Privilege	Important	No	No	2
5011487	高危	March 8, 2022—KB5011487 (OS Builds 19042.1586, 19043.1586, and 19044.1586) for Windows 10,	CVE-2022-24505	Elevation of Privilege	Important	No	No	2
			CVE-2022-24459	Elevation of Privilege	Important	Yes	No	2
			CVE-2022-24507	Elevation of Privilege	Important	No	No	1
			CVE-2022-21975	Denial of Service	Important	No	No	2
			CVE-2022-21967	Elevation of	Important	No	No	2

		version 20H2, all editions ,Windows Server, version 20H2, all editions ,Windows 10, version 21H1, all editions ,Windows 10, version 21H2, all editions		Privilege				
			CVE-2022-23288	Elevation of Privilege	Important	No	No	2
			CVE-2022-23284	Elevation of Privilege	Important	No	No	2
			CVE-2022-23293	Elevation of Privilege	Important	No	No	2
			CVE-2022-23298	Elevation of Privilege	Important	No	No	2
			CVE-2022-21990	Remote Code Execution	Important	Yes	No	1
			CVE-2022-23291	Elevation of Privilege	Important	No	No	2
			CVE-2022-23299	Elevation of Privilege	Important	No	No	1
			CVE-2022-23286	Elevation of Privilege	Important	No	No	1
			CVE-2022-24525	Elevation of Privilege	Important	No	No	2
			CVE-2022-24460	Elevation of Privilege	Important	No	No	2
			CVE-2022-23283	Elevation of Privilege	Important	No	No	2
			CVE-2022-23281	Information Disclosure	Important	No	No	2
			CVE-2022-22010	Information Disclosure	Important	No	No	2
			CVE-2022-24508	Remote Code Execution	Important	No	No	1
			CVE-2022-23287	Elevation of Privilege	Important	No	No	2

			CVE-2022-23297	Information Disclosure	Important	No	No	2
			CVE-2022-24503	Information Disclosure	Important	No	No	2
			CVE-2022-23253	Denial of Service	Important	No	No	1
			CVE-2022-23296	Elevation of Privilege	Important	No	No	2
			CVE-2022-24502	Security Feature Bypass	Important	No	No	1
			CVE-2022-23285	Remote Code Execution	Important	No	No	1
			CVE-2022-23294	Remote Code Execution	Important	No	No	1
			CVE-2022-21977	Information Disclosure	Important	No	No	2
			CVE-2022-23290	Elevation of Privilege	Important	No	No	2
			CVE-2022-24454	Elevation of Privilege	Important	No	No	2
			CVE-2022-23278	Spoofing	Important	No	No	2
5011534	高危	March 8, 2022—KB5011534 (Monthly Rollup) for Windows Server 2008 Service Pack 2	CVE-2022-23299	Elevation of Privilege	Important	No	No	1
			CVE-2022-24459	Elevation of Privilege	Important	Yes	No	2
			CVE-2022-23297	Information Disclosure	Important	No	No	2
			CVE-2022-23290	Elevation of Privilege	Important	No	No	2
			CVE-2022-23283	Elevation of Privilege	Important	No	No	2
			CVE-2022-23281	Information Disclosure	Important	No	No	2
			CVE-2022-23293	Elevation	Important	No	No	2

				of Privilege				
			CVE-2022-23298	Elevation of Privilege	Important	No	No	2
			CVE-2022-23296	Elevation of Privilege	Important	No	No	2
			CVE-2022-24502	Security Feature Bypass	Important	No	No	1
			CVE-2022-21990	Remote Code Execution	Important	Yes	No	1
5011525	高危	March 8, 2022—KB5011525 (Security-only update) for Windows Server 2008 Service Pack 2	CVE-2022-23299	Elevation of Privilege	Important	No	No	1
			CVE-2022-24459	Elevation of Privilege	Important	Yes	No	2
			CVE-2022-23297	Information Disclosure	Important	No	No	2
			CVE-2022-23290	Elevation of Privilege	Important	No	No	2
			CVE-2022-23283	Elevation of Privilege	Important	No	No	2
			CVE-2022-23281	Information Disclosure	Important	No	No	2
			CVE-2022-23293	Elevation of Privilege	Important	No	No	2
			CVE-2022-23298	Elevation of Privilege	Important	No	No	2
			CVE-2022-23296	Elevation of Privilege	Important	No	No	2
			CVE-2022-24502	Security Feature Bypass	Important	No	No	1
			CVE-2022-21990	Remote Code	Important	Yes	No	1

				Execution				
5011493	高危	March 8, 2022—KB5011493 (OS Build 22000.556) for Windows 11	CVE-2022-24505	Elevation of Privilege	Important	No	No	2
			CVE-2022-24459	Elevation of Privilege	Important	Yes	No	2
			CVE-2022-24507	Elevation of Privilege	Important	No	No	1
			CVE-2022-21967	Elevation of Privilege	Important	No	No	2
			CVE-2022-23284	Elevation of Privilege	Important	No	No	2
			CVE-2022-23293	Elevation of Privilege	Important	No	No	2
			CVE-2022-23298	Elevation of Privilege	Important	No	No	2
			CVE-2022-21990	Remote Code Execution	Important	Yes	No	1
			CVE-2022-23291	Elevation of Privilege	Important	No	No	2
			CVE-2022-23299	Elevation of Privilege	Important	No	No	1
			CVE-2022-23286	Elevation of Privilege	Important	No	No	1
			CVE-2022-24525	Elevation of Privilege	Important	No	No	2
			CVE-2022-24460	Elevation of Privilege	Important	No	No	2
			CVE-2022-23283	Elevation of Privilege	Important	No	No	2

			CVE-2022-23281	Information Disclosure	Important	No	No	2
			CVE-2022-22010	Information Disclosure	Important	No	No	2
			CVE-2022-24508	Remote Code Execution	Important	No	No	1
			CVE-2022-23287	Elevation of Privilege	Important	No	No	2
			CVE-2022-23297	Information Disclosure	Important	No	No	2
			CVE-2022-24503	Information Disclosure	Important	No	No	2
			CVE-2022-23253	Denial of Service	Important	No	No	1
			CVE-2022-23296	Elevation of Privilege	Important	No	No	2
			CVE-2022-24502	Security Feature Bypass	Important	No	No	1
			CVE-2022-23294	Remote Code Execution	Important	No	No	1
			CVE-2022-21977	Information Disclosure	Important	No	No	2
			CVE-2022-23290	Elevation of Privilege	Important	No	No	2
			CVE-2022-24454	Elevation of Privilege	Important	No	No	2
			CVE-2022-23278	Spoofing	Important	No	No	2
5011552	高危	March 8, 2022—KB5011552 (Monthly Rollup) for Windows 7 Enterprise	CVE-2022-23285	Remote Code Execution	Important	No	No	1
			CVE-2022-23299	Elevation of Privilege	Important	No	No	1
			CVE-2022-24459	Elevation of Privilege	Important	Yes	No	2
			CVE-2022-23297	Information Disclosure	Important	No	No	2

		ESU,Windows 7 Professional ESU,Windows 7 Ultimate ESU,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-2022-24503	Information Disclosure	Important	No	No	2
			CVE-2022-23283	Elevation of Privilege	Important	No	No	2
			CVE-2022-23290	Elevation of Privilege	Important	No	No	2
			CVE-2022-23253	Denial of Service	Important	No	No	1
			CVE-2022-23281	Information Disclosure	Important	No	No	2
			CVE-2022-23298	Elevation of Privilege	Important	No	No	2
			CVE-2022-23293	Elevation of Privilege	Important	No	No	2
			CVE-2022-23296	Elevation of Privilege	Important	No	No	2
			CVE-2022-21973	Denial of Service	Important	No	No	2
			CVE-2022-24454	Elevation of Privilege	Important	No	No	2
			CVE-2022-24502	Security Feature Bypass	Important	No	No	1
			CVE-2022-21990	Remote Code Execution	Important	Yes	No	1
5011560	高危	March 8, 2022—KB5011560 (Security-only update) for	CVE-2022-24459	Elevation of Privilege	Important	Yes	No	2
			CVE-2022-21975	Denial of Service	Important	No	No	2
			CVE-2022-23284	Elevation of Privilege	Important	No	No	2

		Windows 8.1,Windows Server 2012 R2,Windows Embedded 8.1 Industry Enterprise,Windows Embedded 8.1 Industry Pro	CVE-2022-23293	Elevation of Privilege	Important	No	No	2
			CVE-2022-23298	Elevation of Privilege	Important	No	No	2
			CVE-2022-21990	Remote Code Execution	Important	Yes	No	1
			CVE-2022-23299	Elevation of Privilege	Important	No	No	1
			CVE-2022-23283	Elevation of Privilege	Important	No	No	2
			CVE-2022-23281	Information Disclosure	Important	No	No	2
			CVE-2022-22010	Information Disclosure	Important	No	No	2
			CVE-2022-24455	Elevation of Privilege	Important	No	No	2
			CVE-2022-23297	Information Disclosure	Important	No	No	2
			CVE-2022-24503	Information Disclosure	Important	No	No	2
			CVE-2022-23253	Denial of Service	Important	No	No	1
			CVE-2022-23296	Elevation of Privilege	Important	No	No	2
			CVE-2022-24502	Security Feature Bypass	Important	No	No	1
			CVE-2022-23285	Remote Code Execution	Important	No	No	1
			CVE-2022-23294	Remote Code Execution	Important	No	No	1
			CVE-2022-21977	Information Disclosure	Important	No	No	2
			CVE-2022-23290	Elevation of Privilege	Important	No	No	2

			CVE-2022-21973	Denial of Service	Important	No	No	2
			CVE-2022-24454	Elevation of Privilege	Important	No	No	2
5011564	可选的高危	March 8, 2022—KB5011564 (Monthly Rollup) for Windows 8.1, Windows Server 2012 R2, Windows Embedded 8.1 Industry Enterprise, Windows Embedded 8.1 Industry Pro	CVE-2022-24459	Elevation of Privilege	Important	Yes	No	2
			CVE-2022-21975	Denial of Service	Important	No	No	2
			CVE-2022-23284	Elevation of Privilege	Important	No	No	2
			CVE-2022-23293	Elevation of Privilege	Important	No	No	2
			CVE-2022-23298	Elevation of Privilege	Important	No	No	2
			CVE-2022-21990	Remote Code Execution	Important	Yes	No	1
			CVE-2022-23299	Elevation of Privilege	Important	No	No	1
			CVE-2022-23283	Elevation of Privilege	Important	No	No	2
			CVE-2022-23281	Information Disclosure	Important	No	No	2
			CVE-2022-22010	Information Disclosure	Important	No	No	2
			CVE-2022-24455	Elevation of Privilege	Important	No	No	2
			CVE-2022-23297	Information Disclosure	Important	No	No	2
			CVE-2022-24503	Information Disclosure	Important	No	No	2
			CVE-2022-23253	Denial of Service	Important	No	No	1
			CVE-2022-23296	Elevation of	Important	No	No	2

				Privilege				
			CVE-2022-24502	Security Feature Bypass	Important	No	No	1
			CVE-2022-23285	Remote Code Execution	Important	No	No	1
			CVE-2022-23294	Remote Code Execution	Important	No	No	1
			CVE-2022-21977	Information Disclosure	Important	No	No	2
			CVE-2022-23290	Elevation of Privilege	Important	No	No	2
			CVE-2022-21973	Denial of Service	Important	No	No	2
			CVE-2022-24454	Elevation of Privilege	Important	No	No	2
5011529	高危	March 8, 2022—KB5011529 (Security-only update) for Windows 7 Enterprise ESU, Windows 7 Professional ESU, Windows 7 Ultimate ESU, Windows Server 2008 R2 Enterprise	CVE-2022-23285	Remote Code Execution	Important	No	No	1
			CVE-2022-23299	Elevation of Privilege	Important	No	No	1
			CVE-2022-24459	Elevation of Privilege	Important	Yes	No	2
			CVE-2022-23297	Information Disclosure	Important	No	No	2
			CVE-2022-24503	Information Disclosure	Important	No	No	2
			CVE-2022-23283	Elevation of Privilege	Important	No	No	2
			CVE-2022-23290	Elevation of Privilege	Important	No	No	2
			CVE-2022-23253	Denial of Service	Important	No	No	1
			CVE-2022-23281	Information Disclosure	Important	No	No	2
			CVE-2022-23298	Elevation of	Important	No	No	2

		ESU,Windows Server 2008 R2 Standard ESU,Windows Server 2008 R2 Datacenter ESU,Windows Embedded Standard 7 ESU,Windows Embedded POSReady 7 ESU		Privilege				
			CVE-2022-23293	Elevation of Privilege	Important	No	No	2
			CVE-2022-23296	Elevation of Privilege	Important	No	No	2
			CVE-2022-21973	Denial of Service	Important	No	No	2
			CVE-2022-24454	Elevation of Privilege	Important	No	No	2
			CVE-2022-24502	Security Feature Bypass	Important	No	No	1
			CVE-2022-21990	Remote Code Execution	Important	Yes	No	1

本月微软发布的软件安全更新补丁共 5 个，详细列表如下：

KBID	奇安信集团级别	软件名称	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
5011486	高危	Cumulative security update for Internet Explorer	CVE-2022-23285	Remote Code Execution	Important	No	No	1
			CVE-2022-23299	Elevation of Privilege	Important	No	No	1
			CVE-2022-22010	Information Disclosure	Important	No	No	2
			CVE-2022-21977	Information	Important	No	No	2

				Disclosure				
			CVE-2022-23283	Elevation of Privilege	Important	No	No	2
			CVE-2022-24502	Security Feature Bypass	Important	No	No	1
5012698	高危	Microsoft Exchange Server 2019 and 2016	CVE-2022-23277	Remote Code Execution	Critical	No	No	1
			CVE-2022-24463	Spoofing	Important	No	No	2
5002139	高危	Word 2016	CVE-2022-24511	Tampering	Important	No	No	2
5002068	高危	Word 2013	CVE-2022-24511	Tampering	Important	No	No	2
5010324	高危	Microsoft Exchange Server 2013	CVE-2022-23277	Remote Code Execution	Critical	No	No	1

本月发布内容中还包括 1 个一般性更新补丁：

KBID	奇安信集团级别	详细信息
5002160	其他功能性补丁	Office 2016 更新程序

注：

1、 上述表格中“漏洞的可利用性”编号详细说明如下：

0 - 已被利用(Exploitation Detected)

1 - 更有可能被利用(Exploitation More Likely)

2 - 不太可能利用(Exploitation Less Likely)

3 - 不可能利用(Exploitation Unlikely)

4 - 不受漏洞的影响(N/A)

第5章 参考链接

- Security Update Guide

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

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

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