奇安信集团 2021 年 10 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

2021 年 10月 13 日

目　录

文档信息

文档名称	奇安信集团2021年10月补丁库更新通告		
文档编号	Qi An Xin Group-MSPatch-2021-1001		
发布日期	2021-10-13	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：2021.10.13.1）已发布，本次更新推送了30个微软安全补丁，修复了59个安全漏洞，其中2个微软官方评级为“严重(Critical)”，57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5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 15 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
5006669 5006670 5006667 5006672 5006675	CVE-2021-41338	Security Feature Bypass	Important	Yes	No	Exploitation Less Likely
5006669 5006743 5006670 5006732 5006739 5006714 5006736 5006729 5006728 5006715 5006667 5006672 5006675	CVE-2021-40443	Elevation of Privilege	Important	No	No	Exploitation More Likely
5006669 5006743 5006670 5006732 5006739 5006714 5006736 5006729	CVE-2021-40466	Elevation of Privilege	Important	No	No	Exploitation More Likely

5006728 5006715 5006667 5006672 5006675						
5006669 5006743 5006670 5006732 5006739 5006714 5006736 5006729 5006728 5006715 5006667 5006672 5006675	CVE-2021-40467	Elevation of Privilege	Important	No	No	Exploitation More Likely
5006669 5006743 5006670 5006732 5006739 5006714 5006736 5006729 5006728 5006715 5006667 5006672 5006675	CVE-2021-40449	Elevation of Privilege	Important	No	Yes	Exploitation Detected
5006669 5006670 5006667 5006672 5006675	CVE-2021-40470	Elevation of Privilege	Important	No	No	Exploitation More Likely
5006669 5006743 5006670 5006732 5006739	CVE-2021-40469	Remote Code Execution	Important	Yes	No	Exploitation Less Likely

5006714 5006736 5006729 5006728 5006715 5006672						
5006669 5006743 5006670 5006732 5006739 5006714 5006729 5006728 5006667 5006672 5006675	CVE-2021-41335	Elevation of Privilege	Important	Yes	No	Exploitation Less Likely
5006669 5006743 5006670 5006732 5006739 5006714 5006736 5006729 5006728 5006715 5006667 5006672 5006675	CVE-2021-36970	Spoofing	Important	No	No	Exploitation More Likely
5006670 5006667 5006672	CVE-2021-40461	Remote Code Execution	Critical	No	No	Exploitation Less Likely
5006670	CVE-2021-41357	Elevation of Privilege	Important	No	No	Exploitation More Likely
5006670 5006667 5006672	CVE-2021-40450	Elevation of Privilege	Important	No	No	Exploitation More Likely
5001924 5002004	CVE-2021-40486	Remote Code Execution	Critical	No	No	Exploitation Less Likely

5002036 5002006 5002029 5001960						
5002042 5002029	CVE-2021-41344	Remote Code Execution	Important	No	No	Exploitation More Likely
5002042 5002029	CVE-2021-40487	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 13 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
5006669	高危	October 12, 2021—KB5006669 (OS Build 14393.4704) for Windows 10, version 1607, all editions ,Windows Server 2016, all editions	CVE-2021-41343	Information Disclosure	Important	No	No	2
			CVE-2021-41345	Elevation of Privilege	Important	No	No	2
			CVE-2021-41331	Remote Code Execution	Important	No	No	2
			CVE-2021-41338	Security Feature Bypass	Important	Yes	No	2
			CVE-2021-41332	Information Disclosure	Important	No	No	2
			CVE-2021-40476	Elevation of Privilege	Important	No	No	2
			CVE-2021-40443	Elevation of Privilege	Important	No	No	1
			CVE-2021-40466	Elevation of Privilege	Important	No	No	1
			CVE-2021-40454	Information Disclosure	Important	No	No	2
			CVE-2021-40455	Spoofing	Important	No	No	2
			CVE-2021-40460	Security Feature Bypass	Important	No	No	2
			CVE-2021-40488	Elevation of	Important	No	No	2

				Privilege				
			CVE-2021-36953	Denial of Service	Important	No	No	2
			CVE-2021-40465	Remote Code Execution	Important	No	No	2
			CVE-2021-26442	Elevation of Privilege	Important	No	No	2
			CVE-2021-40467	Elevation of Privilege	Important	No	No	1
			CVE-2021-40449	Elevation of Privilege	Important	No	Yes	0
			CVE-2021-40478	Elevation of Privilege	Important	No	No	2
			CVE-2021-40470	Elevation of Privilege	Important	No	No	1
			CVE-2021-38663	Information Disclosure	Important	No	No	2
			CVE-2021-26441	Elevation of Privilege	Important	No	No	2
			CVE-2021-40477	Elevation of Privilege	Important	No	No	2
			CVE-2021-41347	Elevation of Privilege	Important	No	No	2
			CVE-2021-41342	Remote Code Execution	Important	No	No	2
			CVE-2021-40469	Remote Code Execution	Important	Yes	No	2
			CVE-2021-41335	Elevation of Privilege	Important	Yes	No	2
			CVE-2021-40463	Denial of Service	Important	No	No	2
			CVE-2021-41337	Security Feature	Important	No	No	2

				Bypass				
			CVE-2021-40489	Elevation of Privilege	Important	No	No	2
			CVE-2021-36970	Spoofing	Important	No	No	1
			CVE-2021-38662	Information Disclosure	Important	No	No	2
			CVE-2021-41361	Spoofing	Important	No	No	2
			CVE-2021-41340	Remote Code Execution	Important	No	No	2
5006743	高危	October 12, 2021—KB5006743 (Monthly Rollup) for Windows 7, Windows Server 2008 R2, Windows Embedded Standard 7 ESU, Windows Embedded POSReady 7 ESU, Windows Thin PC	CVE-2021-41343	Information Disclosure	Important	No	No	2
			CVE-2021-41331	Remote Code Execution	Important	No	No	2
			CVE-2021-41332	Information Disclosure	Important	No	No	2
			CVE-2021-40443	Elevation of Privilege	Important	No	No	1
			CVE-2021-40466	Elevation of Privilege	Important	No	No	1
			CVE-2021-40455	Spoofing	Important	No	No	2
			CVE-2021-40460	Security Feature Bypass	Important	No	No	2
			CVE-2021-40465	Remote Code Execution	Important	No	No	2
			CVE-2021-26442	Elevation of Privilege	Important	No	No	2
			CVE-2021-40467	Elevation of Privilege	Important	No	No	1
			CVE-2021-40449	Elevation of Privilege	Important	No	Yes	0
			CVE-2021-38663	Information Disclosure	Important	No	No	2
			CVE-2021-41342	Remote Code Execution	Important	No	No	2

			CVE-2021-40469	Remote Code Execution	Important	Yes	No	2
			CVE-2021-41335	Elevation of Privilege	Important	Yes	No	2
			CVE-2021-40489	Elevation of Privilege	Important	No	No	2
			CVE-2021-38662	Information Disclosure	Important	No	No	2
			CVE-2021-36970	Spoofing	Important	No	No	1
			CVE-2021-36953	Denial of Service	Important	No	No	2
			CVE-2021-41340	Remote Code Execution	Important	No	No	2
5006670	高危	October 12, 2021—KB5006670 (OS Builds 19041.1288, 19042.1288, and 19043.1288) for Windows 10, version 2004, all editions, Windows Server version 2004, Windows 10, version 20H2, all editions, Windows Server,	CVE-2021-41343	Information Disclosure	Important	No	No	2
			CVE-2021-41346	Security Feature Bypass	Important	No	No	2
			CVE-2021-41339	Elevation of Privilege	Important	No	No	2
			CVE-2021-40461	Remote Code Execution	Critical	No	No	2
			CVE-2021-41345	Elevation of Privilege	Important	No	No	2
			CVE-2021-41331	Remote Code Execution	Important	No	No	2
			CVE-2021-41338	Security Feature Bypass	Important	Yes	No	2
			CVE-2021-41332	Information Disclosure	Important	No	No	2
			CVE-2021-40476	Elevation of Privilege	Important	No	No	2
			CVE-2021-40443	Elevation of Privilege	Important	No	No	1
			CVE-2021-40466	Elevation	Important	No	No	1

		version 20H2, all editions ,Windows 10, version 21H1, all editions		of Privilege				
			CVE-2021-40454	Information Disclosure	Important	No	No	2
			CVE-2021-40455	Spoofing	Important	No	No	2
			CVE-2021-40460	Security Feature Bypass	Important	No	No	2
			CVE-2021-41334	Elevation of Privilege	Important	No	No	2
			CVE-2021-40462	Remote Code Execution	Important	No	No	2
			CVE-2021-41357	Elevation of Privilege	Important	No	No	1
			CVE-2021-40488	Elevation of Privilege	Important	No	No	2
			CVE-2021-40475	Information Disclosure	Important	No	No	2
			CVE-2021-40468	Information Disclosure	Important	No	No	2
			CVE-2021-40450	Elevation of Privilege	Important	No	No	1
			CVE-2021-36953	Denial of Service	Important	No	No	2
			CVE-2021-40465	Remote Code Execution	Important	No	No	2
			CVE-2021-26442	Elevation of Privilege	Important	No	No	2
			CVE-2021-40464	Elevation of Privilege	Important	No	No	2
			CVE-2021-41330	Remote Code Execution	Important	No	No	2
			CVE-2021-40467	Elevation of Privilege	Important	No	No	1
			CVE-2021-40449	Elevation	Important	No	Yes	0

				of Privilege				
			CVE-2021-40478	Elevation of Privilege	Important	No	No	2
			CVE-2021-40470	Elevation of Privilege	Important	No	No	1
			CVE-2021-38663	Information Disclosure	Important	No	No	2
			CVE-2021-26441	Elevation of Privilege	Important	No	No	2
			CVE-2021-40477	Elevation of Privilege	Important	No	No	2
			CVE-2021-41347	Elevation of Privilege	Important	No	No	2
			CVE-2021-41342	Remote Code Execution	Important	No	No	2
			CVE-2021-40469	Remote Code Execution	Important	Yes	No	2
			CVE-2021-41335	Elevation of Privilege	Important	Yes	No	2
			CVE-2021-40463	Denial of Service	Important	No	No	2
			CVE-2021-41337	Security Feature Bypass	Important	No	No	2
			CVE-2021-40489	Elevation of Privilege	Important	No	No	2
			CVE-2021-36970	Spoofing	Important	No	No	1
			CVE-2021-38662	Information Disclosure	Important	No	No	2
			CVE-2021-40456	Security Feature Bypass	Important	No	No	2
			CVE-2021-41361	Spoofing	Important	No	No	2
			CVE-2021-41340	Remote Code	Important	No	No	2

				Execution				
5006732	高危	October 12, 2021—KB5006732 (Security-only update) for Windows Server 2012,Windows Embedded 8 Standard	CVE-2021-41343	Information Disclosure	Important	No	No	2
			CVE-2021-41345	Elevation of Privilege	Important	No	No	2
			CVE-2021-41331	Remote Code Execution	Important	No	No	2
			CVE-2021-41332	Information Disclosure	Important	No	No	2
			CVE-2021-40476	Elevation of Privilege	Important	No	No	2
			CVE-2021-40443	Elevation of Privilege	Important	No	No	1
			CVE-2021-36970	Spoofing	Important	No	No	1
			CVE-2021-40466	Elevation of Privilege	Important	No	No	1
			CVE-2021-40454	Information Disclosure	Important	No	No	2
			CVE-2021-40455	Spoofing	Important	No	No	2
			CVE-2021-40460	Security Feature Bypass	Important	No	No	2
			CVE-2021-40488	Elevation of Privilege	Important	No	No	2
			CVE-2021-40465	Remote Code Execution	Important	No	No	2
			CVE-2021-26442	Elevation of Privilege	Important	No	No	2
			CVE-2021-40467	Elevation of Privilege	Important	No	No	1
			CVE-2021-40449	Elevation of Privilege	Important	No	Yes	0
			CVE-2021-40478	Elevation of	Important	No	No	2

				Privilege				
			CVE-2021-38663	Information Disclosure	Important	No	No	2
			CVE-2021-26441	Elevation of Privilege	Important	No	No	2
			CVE-2021-40469	Remote Code Execution	Important	Yes	No	2
			CVE-2021-41335	Elevation of Privilege	Important	Yes	No	2
			CVE-2021-40463	Denial of Service	Important	No	No	2
			CVE-2021-40489	Elevation of Privilege	Important	No	No	2
			CVE-2021-38662	Information Disclosure	Important	No	No	2
			CVE-2021-40477	Elevation of Privilege	Important	No	No	2
			CVE-2021-36953	Denial of Service	Important	No	No	2
			CVE-2021-41340	Remote Code Execution	Important	No	No	2
5006739	可选的高危	October 12, 2021—KB5006739 (Monthly Rollup) for Windows Server 2012, Windows Embedded 8 Standard	CVE-2021-41343	Information Disclosure	Important	No	No	2
			CVE-2021-41345	Elevation of Privilege	Important	No	No	2
			CVE-2021-41331	Remote Code Execution	Important	No	No	2
			CVE-2021-41332	Information Disclosure	Important	No	No	2
			CVE-2021-40476	Elevation of Privilege	Important	No	No	2
			CVE-2021-40443	Elevation of Privilege	Important	No	No	1
			CVE-2021-36970	Spoofing	Important	No	No	1
			CVE-2021-40466	Elevation	Important	No	No	1

				of Privilege				
			CVE-2021-40454	Information Disclosure	Important	No	No	2
			CVE-2021-40455	Spoofing	Important	No	No	2
			CVE-2021-40460	Security Feature Bypass	Important	No	No	2
			CVE-2021-40488	Elevation of Privilege	Important	No	No	2
			CVE-2021-40465	Remote Code Execution	Important	No	No	2
			CVE-2021-26442	Elevation of Privilege	Important	No	No	2
			CVE-2021-40467	Elevation of Privilege	Important	No	No	1
			CVE-2021-40449	Elevation of Privilege	Important	No	Yes	0
			CVE-2021-40478	Elevation of Privilege	Important	No	No	2
			CVE-2021-38663	Information Disclosure	Important	No	No	2
			CVE-2021-26441	Elevation of Privilege	Important	No	No	2
			CVE-2021-41342	Remote Code Execution	Important	No	No	2
			CVE-2021-40469	Remote Code Execution	Important	Yes	No	2
			CVE-2021-41335	Elevation of Privilege	Important	Yes	No	2
			CVE-2021-40463	Denial of Service	Important	No	No	2
			CVE-2021-40489	Elevation of Privilege	Important	No	No	2

			CVE-2021-38662	Information Disclosure	Important	No	No	2
			CVE-2021-40477	Elevation of Privilege	Important	No	No	2
			CVE-2021-36953	Denial of Service	Important	No	No	2
			CVE-2021-41340	Remote Code Execution	Important	No	No	2
5006714	可选的高危	October 12, 2021 — KB5006714 (Monthly Rollup) for Windows 8.1,Windows Server 2012 R2,Windows Embedded 8.1 Industry Enterprise,Windows Embedded 8.1 Industry Pro	CVE-2021-41343	Information Disclosure	Important	No	No	2
			CVE-2021-41345	Elevation of Privilege	Important	No	No	2
			CVE-2021-41331	Remote Code Execution	Important	No	No	2
			CVE-2021-41332	Information Disclosure	Important	No	No	2
			CVE-2021-40476	Elevation of Privilege	Important	No	No	2
			CVE-2021-40443	Elevation of Privilege	Important	No	No	1
			CVE-2021-36970	Spoofing	Important	No	No	1
			CVE-2021-40466	Elevation of Privilege	Important	No	No	1
			CVE-2021-40454	Information Disclosure	Important	No	No	2
			CVE-2021-40455	Spoofing	Important	No	No	2
			CVE-2021-40460	Security Feature Bypass	Important	No	No	2
			CVE-2021-40488	Elevation of Privilege	Important	No	No	2
			CVE-2021-40465	Remote Code Execution	Important	No	No	2
			CVE-2021-26442	Elevation of Privilege	Important	No	No	2

			CVE-2021-40467	Elevation of Privilege	Important	No	No	1
			CVE-2021-40449	Elevation of Privilege	Important	No	Yes	0
			CVE-2021-40478	Elevation of Privilege	Important	No	No	2
			CVE-2021-38663	Information Disclosure	Important	No	No	2
			CVE-2021-26441	Elevation of Privilege	Important	No	No	2
			CVE-2021-41342	Remote Code Execution	Important	No	No	2
			CVE-2021-40469	Remote Code Execution	Important	Yes	No	2
			CVE-2021-41335	Elevation of Privilege	Important	Yes	No	2
			CVE-2021-40463	Denial of Service	Important	No	No	2
			CVE-2021-40489	Elevation of Privilege	Important	No	No	2
			CVE-2021-38662	Information Disclosure	Important	No	No	2
			CVE-2021-40477	Elevation of Privilege	Important	No	No	2
			CVE-2021-36953	Denial of Service	Important	No	No	2
			CVE-2021-41340	Remote Code Execution	Important	No	No	2
5006736	高危	October 12, 2021 — KB5006736 (Monthly Rollup)	CVE-2021-40466	Elevation of Privilege	Important	No	No	1
			CVE-2021-41343	Information Disclosure	Important	No	No	2
			CVE-2021-40465	Remote Code Execution	Important	No	No	2

		for Windows Server 2008	CVE-2021-40449	Elevation of Privilege	Important	No	Yes	0
			CVE-2021-26442	Elevation of Privilege	Important	No	No	2
			CVE-2021-40455	Spoofing	Important	No	No	2
			CVE-2021-41342	Remote Code Execution	Important	No	No	2
			CVE-2021-40469	Remote Code Execution	Important	Yes	No	2
			CVE-2021-41331	Remote Code Execution	Important	No	No	2
			CVE-2021-41332	Information Disclosure	Important	No	No	2
			CVE-2021-40467	Elevation of Privilege	Important	No	No	1
			CVE-2021-40489	Elevation of Privilege	Important	No	No	2
			CVE-2021-40443	Elevation of Privilege	Important	No	No	1
			CVE-2021-36970	Spoofing	Important	No	No	1
			CVE-2021-38662	Information Disclosure	Important	No	No	2
			CVE-2021-36953	Denial of Service	Important	No	No	2
			CVE-2021-41340	Remote Code Execution	Important	No	No	2
			CVE-2021-38663	Information Disclosure	Important	No	No	2
5006729	高危	October 12, 2021—KB5006729 (Security-only update) for	CVE-2021-41343	Information Disclosure	Important	No	No	2
			CVE-2021-41345	Elevation of Privilege	Important	No	No	2
			CVE-2021-41331	Remote Code Execution	Important	No	No	2
			CVE-2021-41332	Information Disclosure	Important	No	No	2

		Windows 8.1,Windows Server 2012 R2,Windows Embedded 8.1 Industry Enterprise,Windows Embedded 8.1 Industry Pro	CVE-2021-40476	Elevation of Privilege	Important	No	No	2
			CVE-2021-40443	Elevation of Privilege	Important	No	No	1
			CVE-2021-36970	Spoofing	Important	No	No	1
			CVE-2021-40466	Elevation of Privilege	Important	No	No	1
			CVE-2021-40454	Information Disclosure	Important	No	No	2
			CVE-2021-40455	Spoofing	Important	No	No	2
			CVE-2021-40460	Security Feature Bypass	Important	No	No	2
			CVE-2021-40488	Elevation of Privilege	Important	No	No	2
			CVE-2021-40465	Remote Code Execution	Important	No	No	2
			CVE-2021-26442	Elevation of Privilege	Important	No	No	2
			CVE-2021-40467	Elevation of Privilege	Important	No	No	1
			CVE-2021-40449	Elevation of Privilege	Important	No	Yes	0
			CVE-2021-40478	Elevation of Privilege	Important	No	No	2
			CVE-2021-38663	Information Disclosure	Important	No	No	2
			CVE-2021-26441	Elevation of Privilege	Important	No	No	2
			CVE-2021-40469	Remote Code Execution	Important	Yes	No	2
			CVE-2021-41335	Elevation of	Important	Yes	No	2

				Privilege				
			CVE-2021-40463	Denial of Service	Important	No	No	2
			CVE-2021-40489	Elevation of Privilege	Important	No	No	2
			CVE-2021-38662	Information Disclosure	Important	No	No	2
			CVE-2021-40477	Elevation of Privilege	Important	No	No	2
			CVE-2021-36953	Denial of Service	Important	No	No	2
			CVE-2021-41340	Remote Code Execution	Important	No	No	2
5006728	高危	October 12, 2021—KB5006728 (Security-only update) for Windows 7, Windows Server 2008 R2, Windows Embedded Standard 7 ESU, Windows Embedded POSReady 7, Windows Thin PC	CVE-2021-41343	Information Disclosure	Important	No	No	2
			CVE-2021-41331	Remote Code Execution	Important	No	No	2
			CVE-2021-41332	Information Disclosure	Important	No	No	2
			CVE-2021-40443	Elevation of Privilege	Important	No	No	1
			CVE-2021-40466	Elevation of Privilege	Important	No	No	1
			CVE-2021-40455	Spoofing	Important	No	No	2
			CVE-2021-40460	Security Feature Bypass	Important	No	No	2
			CVE-2021-40465	Remote Code Execution	Important	No	No	2
			CVE-2021-26442	Elevation of Privilege	Important	No	No	2
			CVE-2021-40467	Elevation of Privilege	Important	No	No	1
			CVE-2021-40449	Elevation of Privilege	Important	No	Yes	0

			CVE-2021-38663	Information Disclosure	Important	No	No	2
			CVE-2021-40469	Remote Code Execution	Important	Yes	No	2
			CVE-2021-41335	Elevation of Privilege	Important	Yes	No	2
			CVE-2021-40489	Elevation of Privilege	Important	No	No	2
			CVE-2021-38662	Information Disclosure	Important	No	No	2
			CVE-2021-36970	Spoofing	Important	No	No	1
			CVE-2021-36953	Denial of Service	Important	No	No	2
			CVE-2021-41340	Remote Code Execution	Important	No	No	2
5006715	高危	October 12, 2021—KB5006715 (Security-only update) for Windows Server 2008	CVE-2021-40466	Elevation of Privilege	Important	No	No	1
			CVE-2021-41343	Information Disclosure	Important	No	No	2
			CVE-2021-40465	Remote Code Execution	Important	No	No	2
			CVE-2021-40449	Elevation of Privilege	Important	No	Yes	0
			CVE-2021-26442	Elevation of Privilege	Important	No	No	2
			CVE-2021-40455	Spoofing	Important	No	No	2
			CVE-2021-40469	Remote Code Execution	Important	Yes	No	2
			CVE-2021-41331	Remote Code Execution	Important	No	No	2
			CVE-2021-41332	Information Disclosure	Important	No	No	2
			CVE-2021-40467	Elevation of Privilege	Important	No	No	1
			CVE-2021-40489	Elevation of	Important	No	No	2

				Privilege				
			CVE-2021-40443	Elevation of Privilege	Important	No	No	1
			CVE-2021-36970	Spoofing	Important	No	No	1
			CVE-2021-38662	Information Disclosure	Important	No	No	2
			CVE-2021-36953	Denial of Service	Important	No	No	2
			CVE-2021-41340	Remote Code Execution	Important	No	No	2
			CVE-2021-38663	Information Disclosure	Important	No	No	2
5006667	高危	October 12, 2021—KB5006667 (OS Build 18363.1854) for Windows 10 Enterprise, version 1909, Windows 10 Enterprise and Education, version 1909, Windows 10 IoT Enterprise, version 1909	CVE-2021-41343	Information Disclosure	Important	No	No	2
			CVE-2021-41339	Elevation of Privilege	Important	No	No	2
			CVE-2021-40461	Remote Code Execution	Critical	No	No	2
			CVE-2021-41345	Elevation of Privilege	Important	No	No	2
			CVE-2021-41331	Remote Code Execution	Important	No	No	2
			CVE-2021-41338	Security Feature Bypass	Important	Yes	No	2
			CVE-2021-41332	Information Disclosure	Important	No	No	2
			CVE-2021-40476	Elevation of Privilege	Important	No	No	2
			CVE-2021-40443	Elevation of Privilege	Important	No	No	1
			CVE-2021-40466	Elevation of Privilege	Important	No	No	1
			CVE-2021-40454	Information Disclosure	Important	No	No	2
			CVE-2021-40455	Spoofing	Important	No	No	2

			CVE-2021-40460	Security Feature Bypass	Important	No	No	2
			CVE-2021-40462	Remote Code Execution	Important	No	No	2
			CVE-2021-40488	Elevation of Privilege	Important	No	No	2
			CVE-2021-40475	Information Disclosure	Important	No	No	2
			CVE-2021-40450	Elevation of Privilege	Important	No	No	1
			CVE-2021-40465	Remote Code Execution	Important	No	No	2
			CVE-2021-26442	Elevation of Privilege	Important	No	No	2
			CVE-2021-40464	Elevation of Privilege	Important	No	No	2
			CVE-2021-41330	Remote Code Execution	Important	No	No	2
			CVE-2021-40467	Elevation of Privilege	Important	No	No	1
			CVE-2021-40449	Elevation of Privilege	Important	No	Yes	0
			CVE-2021-40478	Elevation of Privilege	Important	No	No	2
			CVE-2021-40470	Elevation of Privilege	Important	No	No	1
			CVE-2021-38663	Information Disclosure	Important	No	No	2
			CVE-2021-26441	Elevation of Privilege	Important	No	No	2
			CVE-2021-40477	Elevation of	Important	No	No	2

				Privilege				
			CVE-2021-41347	Elevation of Privilege	Important	No	No	2
			CVE-2021-41342	Remote Code Execution	Important	No	No	2
			CVE-2021-41335	Elevation of Privilege	Important	Yes	No	2
			CVE-2021-40463	Denial of Service	Important	No	No	2
			CVE-2021-40489	Elevation of Privilege	Important	No	No	2
			CVE-2021-38662	Information Disclosure	Important	No	No	2
			CVE-2021-36970	Spoofing	Important	No	No	1
			CVE-2021-36953	Denial of Service	Important	No	No	2
			CVE-2021-41340	Remote Code Execution	Important	No	No	2
5006672	高危	October 12, 2021—KB5006672 (OS Build 17763.2237) for Windows 10 Enterprise 2019 LTSC, Windows 10 IoT Enterprise 2019 LTSC, Windows 10 IoT Core 2019 LTSC	CVE-2021-41343	Information Disclosure	Important	No	No	2
			CVE-2021-40461	Remote Code Execution	Critical	No	No	2
			CVE-2021-41345	Elevation of Privilege	Important	No	No	2
			CVE-2021-41331	Remote Code Execution	Important	No	No	2
			CVE-2021-41338	Security Feature Bypass	Important	Yes	No	2
			CVE-2021-41332	Information Disclosure	Important	No	No	2
			CVE-2021-40476	Elevation of Privilege	Important	No	No	2
			CVE-2021-40443	Elevation of Privilege	Important	No	No	1
			CVE-2021-40466	Elevation	Important	No	No	1

				of Privilege				
			CVE-2021-40454	Information Disclosure	Important	No	No	2
			CVE-2021-40455	Spoofing	Important	No	No	2
			CVE-2021-40460	Security Feature Bypass	Important	No	No	2
			CVE-2021-40462	Remote Code Execution	Important	No	No	2
			CVE-2021-40488	Elevation of Privilege	Important	No	No	2
			CVE-2021-40475	Information Disclosure	Important	No	No	2
			CVE-2021-40450	Elevation of Privilege	Important	No	No	1
			CVE-2021-40465	Remote Code Execution	Important	No	No	2
			CVE-2021-26442	Elevation of Privilege	Important	No	No	2
			CVE-2021-40464	Elevation of Privilege	Important	No	No	2
			CVE-2021-41361	Spoofing	Important	No	No	2
			CVE-2021-41330	Remote Code Execution	Important	No	No	2
			CVE-2021-40467	Elevation of Privilege	Important	No	No	1
			CVE-2021-40449	Elevation of Privilege	Important	No	Yes	0
			CVE-2021-40478	Elevation of Privilege	Important	No	No	2
			CVE-2021-40470	Elevation of Privilege	Important	No	No	1
			CVE-2021-38663	Information	Important	No	No	2

				Disclosure				
			CVE-2021-26441	Elevation of Privilege	Important	No	No	2
			CVE-2021-40477	Elevation of Privilege	Important	No	No	2
			CVE-2021-41347	Elevation of Privilege	Important	No	No	2
			CVE-2021-41342	Remote Code Execution	Important	No	No	2
			CVE-2021-40469	Remote Code Execution	Important	Yes	No	2
			CVE-2021-41335	Elevation of Privilege	Important	Yes	No	2
			CVE-2021-40463	Denial of Service	Important	No	No	2
			CVE-2021-41337	Security Feature Bypass	Important	No	No	2
			CVE-2021-40489	Elevation of Privilege	Important	No	No	2
			CVE-2021-36970	Spoofing	Important	No	No	1
			CVE-2021-38662	Information Disclosure	Important	No	No	2
			CVE-2021-40456	Security Feature Bypass	Important	No	No	2
			CVE-2021-36953	Denial of Service	Important	No	No	2
			CVE-2021-41340	Remote Code Execution	Important	No	No	2
5006675	高危	October 12, 2021 — KB5006675 (OS Build 10240.19	CVE-2021-41343	Information Disclosure	Important	No	No	2
			CVE-2021-41345	Elevation of Privilege	Important	No	No	2
			CVE-2021-41331	Remote Code Execution	Important	No	No	2

		086) for Windows 10	CVE-2021-41338	Security Feature Bypass	Important	Yes	No	2
			CVE-2021-41332	Information Disclosure	Important	No	No	2
			CVE-2021-40476	Elevation of Privilege	Important	No	No	2
			CVE-2021-40443	Elevation of Privilege	Important	No	No	1
			CVE-2021-36970	Spoofing	Important	No	No	1
			CVE-2021-40466	Elevation of Privilege	Important	No	No	1
			CVE-2021-40454	Information Disclosure	Important	No	No	2
			CVE-2021-40455	Spoofing	Important	No	No	2
			CVE-2021-40460	Security Feature Bypass	Important	No	No	2
			CVE-2021-40488	Elevation of Privilege	Important	No	No	2
			CVE-2021-40465	Remote Code Execution	Important	No	No	2
			CVE-2021-26442	Elevation of Privilege	Important	No	No	2
			CVE-2021-40467	Elevation of Privilege	Important	No	No	1
			CVE-2021-40449	Elevation of Privilege	Important	No	Yes	0
			CVE-2021-40478	Elevation of Privilege	Important	No	No	2
			CVE-2021-40470	Elevation of Privilege	Important	No	No	1
			CVE-2021-38663	Information	Important	No	No	2

				Disclosure				
			CVE-2021-26441	Elevation of Privilege	Important	No	No	2
			CVE-2021-41347	Elevation of Privilege	Important	No	No	2
			CVE-2021-41342	Remote Code Execution	Important	No	No	2
			CVE-2021-41335	Elevation of Privilege	Important	Yes	No	2
			CVE-2021-40463	Denial of Service	Important	No	No	2
			CVE-2021-40489	Elevation of Privilege	Important	No	No	2
			CVE-2021-38662	Information Disclosure	Important	No	No	2
			CVE-2021-40477	Elevation of Privilege	Important	No	No	2
			CVE-2021-36953	Denial of Service	Important	No	No	2
			CVE-2021-41340	Remote Code Execution	Important	No	No	2

本月微软发布的软件安全更新补丁共 17 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
5007011	高危	Exchange Server 2013	CVE-2021-26427	Remote Code Execution	Important	No	No	2
4018332	高危	Office 2013	CVE-2021-40454	Information Disclosure	Important	No	No	2

4461476	高危	Office 2016	CVE-2021-40454	Information Disclosure	Important	No	No	2
4493202	高危	Enterprise Server 2013	CVE-2021-40485	Remote Code Execution	Important	No	No	2
5002029	高危	SharePoint Enterprise Server 2016	CVE-2021-40486	Remote Code Execution	Critical	No	No	2
			CVE-2021-40484	Spoofing	Important	No	No	2
			CVE-2021-41344	Remote Code Execution	Important	No	No	1
			CVE-2021-40487	Remote Code Execution	Important	No	No	1
5001985	高危	Office 2013	CVE-2021-40471	Remote Code Execution	Important	No	No	2
			CVE-2021-40473	Remote Code Execution	Important	No	No	2
			CVE-2021-40472	Information Disclosure	Important	No	No	2
			CVE-2021-40479	Remote Code Execution	Important	No	No	2
5001960	高危	Word 2013	CVE-2021-40486	Remote Code Execution	Critical	No	No	2
5002006	高危	SharePoint Enterprise Server 2016	CVE-2021-40486	Remote Code Execution	Critical	No	No	2
5002030	高危	Excel 2016	CVE-2021-40485	Remote Code Execution	Important	No	No	2
			CVE-2021-40472	Information Disclosure	Important	No	No	2
			CVE-2021-40474	Remote Code	Important	No	No	2

				Execution				
5002042	高危	SharePoint Foundation 2013	CVE-2021-40484	Spoofing	Important	No	No	2
			CVE-2021-41344	Remote Code Execution	Important	No	No	1
			CVE-2021-40487	Remote Code Execution	Important	No	No	1
5001924	高危	SharePoint Enterprise Server 2013	CVE-2021-40486	Remote Code Execution	Critical	No	No	2
5002004	高危	Word 2016	CVE-2021-40486	Remote Code Execution	Critical	No	No	2
5007012	高危	Exchange Server 2019 and 2016	CVE-2021-26427	Remote Code Execution	Important	No	No	2
			CVE-2021-41350	Spoofing	Important	No	No	2
			CVE-2021-41348	Elevation of Privilege	Important	No	No	2
			CVE-2021-34453	Denial of Service	Important	No	No	2
5002036	高危	Office Web Apps Server 2013	CVE-2021-40486	Remote Code Execution	Critical	No	No	2
			CVE-2021-40472	Information Disclosure	Important	No	No	2
			CVE-2021-40474	Remote Code Execution	Important	No	No	2
5001982	高危	Office 2016	CVE-2021-40471	Remote Code Execution	Important	No	No	2
			CVE-2021-40473	Remote Code Execution	Important	No	No	2
			CVE-2021-40472	Information Disclosure	Important	No	No	2
			CVE-2021-40479	Remote	Important	No	No	2

				Code Execution				
5002043	高危	Excel 2013	CVE-2021-40485	Remote Code Execution	Important	No	No	2
			CVE-2021-40472	Information Disclosure	Important	No	No	2
			CVE-2021-40474	Remote Code Execution	Important	No	No	2
5006671	高危	Internet Explorer	CVE-2021-41342	Remote Code Execution	Important	No	No	2

本月发布内容中还包括 5 个一般性更新补丁：

KBID	奇安信集团级别	详细信息
5001978	其他功能性补丁	Access 2016 更新程序
3114524	其他功能性补丁	Office 2016 更新程序
4462197	其他功能性补丁	Office 2016 更新程序
4486711	其他功能性补丁	Office 2016 更新程序
5001998	其他功能性补丁	Outlook 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