奇安信集团 2021 年 09 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 09月 15 日

目　录

文档信息

文档名称	奇安信集团 2021 年 09 月补丁库更新通告		
文档编号	Qi An Xin Group-MSPatch-2021-0901		
发布日期	2021-09-15	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：2021.09.15.1）已发布，本次更新推送了25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
5005566	CVE-2021-36958	Remote Code Execution	Important	Yes	No	Exploitation More Likely
5005615						
5005613						
5005606						
5005627						
5005623						
5005633						
5005569						
5005565						
5005573						
5005607						
5005568						
5005618						
5005566	CVE-2021-38633	Elevation of Privilege	Important	No	No	Exploitation More Likely
5005615						
5005613						
5005606						
5005627						
5005623						
5005633						
5005569						
5005565						
5005573						
5005607						
5005568						
5005618						

5005566 5005615 5005613 5005606 5005627 5005623 5005633 5005569 5005565 5005573 5005607 5005568 5005618	CVE-2021-36963	Elevation of Privilege	Important	No	No	Exploitation More Likely
5005566 5005565 5005568	CVE-2021-36975	Elevation of Privilege	Important	No	No	Exploitation More Likely
5005566 5005615 5005613 5005606 5005627 5005623 5005633 5005569 5005565 5005573 5005607 5005568 5005618	CVE-2021-36965	Remote Code Execution	Critical	No	No	Exploitation Less Likely
5005566 5005615 5005613 5005606 5005627 5005623 5005633 5005569 5005565 5005573 5005607 5005568	CVE-2021-26435	Remote Code Execution	Critical	No	No	Exploitation Less Likely

5005566 5005615 5005613 5005606 5005627 5005623 5005633 5005569 5005565 5005573 5005607 5005568 5005618	CVE-2021-36955	Elevation of Privilege	Important	No	No	Exploitation More Likely
5005566 5005615 5005613 5005606 5005627 5005623 5005633 5005569 5005565 5005573 5005607 5005568 5005618	CVE-2021-38639	Elevation of Privilege	Important	No	No	Exploitation More Likely
5005566 5005563 5005613 5005606 5005627 5005623 5005633 5005569 5005565 5005573 5005568	CVE-2021-40444	Remote Code Execution	Important	Yes	Yes	Exploitation Detected
5005566 5005615 5005613 5005606	CVE-2021-38671	Elevation of Privilege	Important	No	No	Exploitation More Likely

5005627 5005623 5005633 5005569 5005565 5005573 5005607 5005568 5005618						
5005615 5005606 5005633 5005618	CVE-2021-36968	Elevation of Privilege	Important	Yes	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 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
5005566	高危	September 14, 2021—KB5005566 (OS Build 18363.1801) for Windows 10 Enterprise, version 1909, Windows 10 Enterprise and Education, version 1909, Windows 10 IoT Enterprise, version 1909	CVE-2021-36958	Remote Code Execution	Important	Yes	No	1
			CVE-2021-36966	Elevation of Privilege	Important	No	No	2
			CVE-2021-36969	Information Disclosure	Important	No	No	2
			CVE-2021-38633	Elevation of Privilege	Important	No	No	1
			CVE-2021-38634	Elevation of Privilege	Important	No	No	2
			CVE-2021-36963	Elevation of Privilege	Important	No	No	1
			CVE-2021-36975	Elevation of Privilege	Important	No	No	1
			CVE-2021-38638	Elevation of Privilege	Important	No	No	2
			CVE-2021-36973	Elevation of Privilege	Important	No	No	2
			CVE-2021-36965	Remote Code Execution	Critical	No	No	2
			CVE-2021-36962	Information Disclosure	Important	No	No	2

			CVE-2021-38630	Elevation of Privilege	Important	No	No	2
			CVE-2021-36967	Elevation of Privilege	Important	No	No	2
			CVE-2021-26435	Remote Code Execution	Critical	No	No	2
			CVE-2021-36964	Elevation of Privilege	Important	No	No	2
			CVE-2021-36955	Elevation of Privilege	Important	No	No	1
			CVE-2021-38667	Elevation of Privilege	Important	No	No	2
			CVE-2021-38628	Elevation of Privilege	Important	No	No	2
			CVE-2021-36961	Denial of Service	Important	No	No	2
			CVE-2021-36960	Information Disclosure	Important	No	No	2
			CVE-2021-38639	Elevation of Privilege	Important	No	No	1
			CVE-2021-36972	Information Disclosure	Important	No	No	2
			CVE-2021-38629	Information Disclosure	Important	No	No	2
			CVE-2021-36954	Elevation of Privilege	Important	No	No	2
			CVE-2021-40444	Remote Code Execution	Important	Yes	Yes	0
			CVE-2021-38635	Information Disclosure	Important	No	No	2
			CVE-2021-38636	Information Disclosure	Important	No	No	2
			CVE-2021-36974	Elevation of	Important	No	No	2

				Privilege				
			CVE-2021-36959	Spoofing	Important	No	No	2
			CVE-2021-38637	Information Disclosure	Important	No	No	2
			CVE-2021-40447	Elevation of Privilege	Important	No	No	2
			CVE-2021-38671	Elevation of Privilege	Important	No	No	1
			CVE-2021-38632	Security Feature Bypass	Important	No	No	2
			CVE-2021-38624	Security Feature Bypass	Important	No	No	2
5005615	高危	September 14, 2021—KB5005615 (Security-only update) for Windows 7, Windows Server 2008 R2, Windows Embedded Standard 7 ESU, Windows Embedded POSReady 7 ESU, Windows Thin PC	CVE-2021-36958	Remote Code Execution	Important	Yes	No	1
			CVE-2021-36969	Information Disclosure	Important	No	No	2
			CVE-2021-38633	Elevation of Privilege	Important	No	No	1
			CVE-2021-36963	Elevation of Privilege	Important	No	No	1
			CVE-2021-38638	Elevation of Privilege	Important	No	No	2
			CVE-2021-36965	Remote Code Execution	Critical	No	No	2
			CVE-2021-38630	Elevation of Privilege	Important	No	No	2
			CVE-2021-26435	Remote Code Execution	Critical	No	No	2
			CVE-2021-36964	Elevation of Privilege	Important	No	No	2
			CVE-2021-36955	Elevation of Privilege	Important	No	No	1

			CVE-2021-38667	Elevation of Privilege	Important	No	No	2
			CVE-2021-36959	Spoofing	Important	No	No	2
			CVE-2021-38628	Elevation of Privilege	Important	No	No	2
			CVE-2021-36961	Denial of Service	Important	No	No	2
			CVE-2021-36960	Information Disclosure	Important	No	No	2
			CVE-2021-36968	Elevation of Privilege	Important	Yes	No	2
			CVE-2021-38639	Elevation of Privilege	Important	No	No	1
			CVE-2021-38635	Information Disclosure	Important	No	No	2
			CVE-2021-38636	Information Disclosure	Important	No	No	2
			CVE-2021-36962	Information Disclosure	Important	No	No	2
			CVE-2021-38629	Information Disclosure	Important	No	No	2
			CVE-2021-40447	Elevation of Privilege	Important	No	No	2
			CVE-2021-38671	Elevation of Privilege	Important	No	No	1
5005613	高危	September 14, 2021—KB5005613 (Monthly Rollup) for Windows 8.1, Windows	CVE-2021-36958	Remote Code Execution	Important	Yes	No	1
			CVE-2021-36969	Information Disclosure	Important	No	No	2
			CVE-2021-38633	Elevation of Privilege	Important	No	No	1
			CVE-2021-36963	Elevation of Privilege	Important	No	No	1
			CVE-2021-38638	Elevation	Important	No	No	2

		Server 2012 R2,Windows Embedded 8.1 Industry Enterprise,Windows Embedded 8.1 Industry Pro		of Privilege				
			CVE-2021-36962	Information Disclosure	Important	No	No	2
			CVE-2021-36965	Remote Code Execution	Critical	No	No	2
			CVE-2021-38630	Elevation of Privilege	Important	No	No	2
			CVE-2021-26435	Remote Code Execution	Critical	No	No	2
			CVE-2021-36964	Elevation of Privilege	Important	No	No	2
			CVE-2021-36955	Elevation of Privilege	Important	No	No	1
			CVE-2021-38667	Elevation of Privilege	Important	No	No	2
			CVE-2021-36959	Spoofing	Important	No	No	2
			CVE-2021-38628	Elevation of Privilege	Important	No	No	2
			CVE-2021-36961	Denial of Service	Important	No	No	2
			CVE-2021-36960	Information Disclosure	Important	No	No	2
			CVE-2021-38639	Elevation of Privilege	Important	No	No	1
			CVE-2021-36972	Information Disclosure	Important	No	No	2
			CVE-2021-40444	Remote Code Execution	Important	Yes	Yes	0
			CVE-2021-38635	Information Disclosure	Important	No	No	2
			CVE-2021-38636	Information Disclosure	Important	No	No	2
			CVE-2021-36974	Elevation of Privilege	Important	No	No	2

			CVE-2021-38629	Information Disclosure	Important	No	No	2
			CVE-2021-40447	Elevation of Privilege	Important	No	No	2
			CVE-2021-38671	Elevation of Privilege	Important	No	No	1
			CVE-2021-38624	Security Feature Bypass	Important	No	No	2
5005606	高危	September 14, 2021—KB5005606 (Monthly Rollup) for Windows Server 2008	CVE-2021-36958	Remote Code Execution	Important	Yes	No	1
			CVE-2021-38633	Elevation of Privilege	Important	No	No	1
			CVE-2021-36963	Elevation of Privilege	Important	No	No	1
			CVE-2021-38626	Elevation of Privilege	Important	No	No	2
			CVE-2021-38638	Elevation of Privilege	Important	No	No	2
			CVE-2021-36965	Remote Code Execution	Critical	No	No	2
			CVE-2021-26435	Remote Code Execution	Critical	No	No	2
			CVE-2021-36964	Elevation of Privilege	Important	No	No	2
			CVE-2021-36955	Elevation of Privilege	Important	No	No	1
			CVE-2021-38667	Elevation of Privilege	Important	No	No	2
			CVE-2021-36959	Spoofing	Important	No	No	2
			CVE-2021-38628	Elevation of Privilege	Important	No	No	2

			CVE-2021-38625	Elevation of Privilege	Important	No	No	2
			CVE-2021-36961	Denial of Service	Important	No	No	2
			CVE-2021-36968	Elevation of Privilege	Important	Yes	No	2
			CVE-2021-38639	Elevation of Privilege	Important	No	No	1
			CVE-2021-40444	Remote Code Execution	Important	Yes	Yes	0
			CVE-2021-38635	Information Disclosure	Important	No	No	2
			CVE-2021-38636	Information Disclosure	Important	No	No	2
			CVE-2021-36962	Information Disclosure	Important	No	No	2
			CVE-2021-38629	Information Disclosure	Important	No	No	2
			CVE-2021-40447	Elevation of Privilege	Important	No	No	2
			CVE-2021-38671	Elevation of Privilege	Important	No	No	1
5005627	高危	September 14, 2021—KB5005627 (Security-only update) for Windows 8.1, Windows Server 2012 R2, Windo	CVE-2021-36958	Remote Code Execution	Important	Yes	No	1
			CVE-2021-36969	Information Disclosure	Important	No	No	2
			CVE-2021-38633	Elevation of Privilege	Important	No	No	1
			CVE-2021-36963	Elevation of Privilege	Important	No	No	1
			CVE-2021-38638	Elevation of Privilege	Important	No	No	2
			CVE-2021-36962	Information Disclosure	Important	No	No	2

		ws Embedded 8.1 Industry Enterprise,Windows Embedded 8.1 Industry Pro	CVE-2021-36965	Remote Code Execution	Critical	No	No	2
			CVE-2021-38630	Elevation of Privilege	Important	No	No	2
			CVE-2021-26435	Remote Code Execution	Critical	No	No	2
			CVE-2021-36964	Elevation of Privilege	Important	No	No	2
			CVE-2021-36955	Elevation of Privilege	Important	No	No	1
			CVE-2021-38667	Elevation of Privilege	Important	No	No	2
			CVE-2021-36959	Spoofing	Important	No	No	2
			CVE-2021-38628	Elevation of Privilege	Important	No	No	2
			CVE-2021-36961	Denial of Service	Important	No	No	2
			CVE-2021-36960	Information Disclosure	Important	No	No	2
			CVE-2021-38639	Elevation of Privilege	Important	No	No	1
			CVE-2021-36972	Information Disclosure	Important	No	No	2
			CVE-2021-40444	Remote Code Execution	Important	Yes	Yes	0
			CVE-2021-38635	Information Disclosure	Important	No	No	2
			CVE-2021-38636	Information Disclosure	Important	No	No	2
			CVE-2021-36974	Elevation of Privilege	Important	No	No	2
			CVE-2021-38629	Information Disclosure	Important	No	No	2
			CVE-2021-40447	Elevation of	Important	No	No	2

				Privilege				
			CVE-2021-38671	Elevation of Privilege	Important	No	No	1
			CVE-2021-38624	Security Feature Bypass	Important	No	No	2
5005623	高危	September 14, 2021—KB5005623 (Monthly Rollup) for Windows Server 2012,Windows Embedded 8 Standard	CVE-2021-36958	Remote Code Execution	Important	Yes	No	1
			CVE-2021-36969	Information Disclosure	Important	No	No	2
			CVE-2021-38633	Elevation of Privilege	Important	No	No	1
			CVE-2021-36963	Elevation of Privilege	Important	No	No	1
			CVE-2021-38638	Elevation of Privilege	Important	No	No	2
			CVE-2021-36962	Information Disclosure	Important	No	No	2
			CVE-2021-36965	Remote Code Execution	Critical	No	No	2
			CVE-2021-26435	Remote Code Execution	Critical	No	No	2
			CVE-2021-36964	Elevation of Privilege	Important	No	No	2
			CVE-2021-36955	Elevation of Privilege	Important	No	No	1
			CVE-2021-38667	Elevation of Privilege	Important	No	No	2
			CVE-2021-36959	Spoofing	Important	No	No	2
			CVE-2021-38628	Elevation of Privilege	Important	No	No	2
			CVE-2021-36961	Denial of Service	Important	No	No	2
			CVE-2021-36960	Information	Important	No	No	2

				Disclosure				
			CVE-2021-38639	Elevation of Privilege	Important	No	No	1
			CVE-2021-36972	Information Disclosure	Important	No	No	2
			CVE-2021-40444	Remote Code Execution	Important	Yes	Yes	0
			CVE-2021-38635	Information Disclosure	Important	No	No	2
			CVE-2021-38636	Information Disclosure	Important	No	No	2
			CVE-2021-36974	Elevation of Privilege	Important	No	No	2
			CVE-2021-38629	Information Disclosure	Important	No	No	2
			CVE-2021-40447	Elevation of Privilege	Important	No	No	2
			CVE-2021-38671	Elevation of Privilege	Important	No	No	1
5005633	高危	September 14, 2021—KB5005633 (Monthly Rollup) for Windows 7, Windows Server 2008 R2, Windows Embedded Standard 7 ESU, Windows	CVE-2021-36958	Remote Code Execution	Important	Yes	No	1
			CVE-2021-36969	Information Disclosure	Important	No	No	2
			CVE-2021-38633	Elevation of Privilege	Important	No	No	1
			CVE-2021-36963	Elevation of Privilege	Important	No	No	1
			CVE-2021-38638	Elevation of Privilege	Important	No	No	2
			CVE-2021-36965	Remote Code Execution	Critical	No	No	2
			CVE-2021-38630	Elevation of Privilege	Important	No	No	2
			CVE-2021-26435	Remote Code	Critical	No	No	2

		Embedded POSReady 7 ESU,Windows Thin PC		Execution				
			CVE-2021-36964	Elevation of Privilege	Important	No	No	2
			CVE-2021-36955	Elevation of Privilege	Important	No	No	1
			CVE-2021-38667	Elevation of Privilege	Important	No	No	2
			CVE-2021-36959	Spoofing	Important	No	No	2
			CVE-2021-38628	Elevation of Privilege	Important	No	No	2
			CVE-2021-36961	Denial of Service	Important	No	No	2
			CVE-2021-36960	Information Disclosure	Important	No	No	2
			CVE-2021-36968	Elevation of Privilege	Important	Yes	No	2
			CVE-2021-38639	Elevation of Privilege	Important	No	No	1
			CVE-2021-40444	Remote Code Execution	Important	Yes	Yes	0
			CVE-2021-38635	Information Disclosure	Important	No	No	2
			CVE-2021-38636	Information Disclosure	Important	No	No	2
			CVE-2021-36962	Information Disclosure	Important	No	No	2
			CVE-2021-38629	Information Disclosure	Important	No	No	2
			CVE-2021-40447	Elevation of Privilege	Important	No	No	2
			CVE-2021-38671	Elevation of Privilege	Important	No	No	1
5005569	高危	September 14,	CVE-2021-36958	Remote Code Execution	Important	Yes	No	1

		2021—KB5005569 (OS Build 10240.19060) for Windows 10	CVE-2021-36969	Information Disclosure	Important	No	No	2
			CVE-2021-38633	Elevation of Privilege	Important	No	No	1
			CVE-2021-38634	Elevation of Privilege	Important	No	No	2
			CVE-2021-36963	Elevation of Privilege	Important	No	No	1
			CVE-2021-38638	Elevation of Privilege	Important	No	No	2
			CVE-2021-36973	Elevation of Privilege	Important	No	No	2
			CVE-2021-36965	Remote Code Execution	Critical	No	No	2
			CVE-2021-36962	Information Disclosure	Important	No	No	2
			CVE-2021-38630	Elevation of Privilege	Important	No	No	2
			CVE-2021-36967	Elevation of Privilege	Important	No	No	2
			CVE-2021-26435	Remote Code Execution	Critical	No	No	2
			CVE-2021-36964	Elevation of Privilege	Important	No	No	2
			CVE-2021-36955	Elevation of Privilege	Important	No	No	1
			CVE-2021-38667	Elevation of Privilege	Important	No	No	2
			CVE-2021-38628	Elevation of Privilege	Important	No	No	2
			CVE-2021-36961	Denial of	Important	No	No	2

				Service				
			CVE-2021-36960	Information Disclosure	Important	No	No	2
			CVE-2021-38639	Elevation of Privilege	Important	No	No	1
			CVE-2021-36972	Information Disclosure	Important	No	No	2
			CVE-2021-38629	Information Disclosure	Important	No	No	2
			CVE-2021-40444	Remote Code Execution	Important	Yes	Yes	0
			CVE-2021-38635	Information Disclosure	Important	No	No	2
			CVE-2021-38636	Information Disclosure	Important	No	No	2
			CVE-2021-36974	Elevation of Privilege	Important	No	No	2
			CVE-2021-36959	Spoofing	Important	No	No	2
			CVE-2021-40447	Elevation of Privilege	Important	No	No	2
			CVE-2021-38671	Elevation of Privilege	Important	No	No	1
			CVE-2021-38624	Security Feature Bypass	Important	No	No	2
5005565	高危	September 14, 2021—KB5005565 (OS Builds 19041.1237, 19042.1237, and 19043.1237) for Windows	CVE-2021-36958	Remote Code Execution	Important	Yes	No	1
			CVE-2021-36966	Elevation of Privilege	Important	No	No	2
			CVE-2021-36969	Information Disclosure	Important	No	No	2
			CVE-2021-38633	Elevation of Privilege	Important	No	No	1
			CVE-2021-38634	Elevation of Privilege	Important	No	No	2

		10, version 2004, all editions ,Windows Server version 2004,Windows 10, version 20H2, all editions ,Windows Server, version 20H2, all editions ,Windows 10, version 21H1, all editions	CVE-2021-36963	Elevation of Privilege	Important	No	No	1
			CVE-2021-36975	Elevation of Privilege	Important	No	No	1
			CVE-2021-38638	Elevation of Privilege	Important	No	No	2
			CVE-2021-36973	Elevation of Privilege	Important	No	No	2
			CVE-2021-36965	Remote Code Execution	Critical	No	No	2
			CVE-2021-36962	Information Disclosure	Important	No	No	2
			CVE-2021-38630	Elevation of Privilege	Important	No	No	2
			CVE-2021-36967	Elevation of Privilege	Important	No	No	2
			CVE-2021-26435	Remote Code Execution	Critical	No	No	2
			CVE-2021-36964	Elevation of Privilege	Important	No	No	2
			CVE-2021-36955	Elevation of Privilege	Important	No	No	1
			CVE-2021-38667	Elevation of Privilege	Important	No	No	2
			CVE-2021-38628	Elevation of Privilege	Important	No	No	2
			CVE-2021-36961	Denial of Service	Important	No	No	2
			CVE-2021-36960	Information Disclosure	Important	No	No	2
			CVE-2021-38639	Elevation of	Important	No	No	1

				Privilege				
			CVE-2021-36972	Information Disclosure	Important	No	No	2
			CVE-2021-38629	Information Disclosure	Important	No	No	2
			CVE-2021-36954	Elevation of Privilege	Important	No	No	2
			CVE-2021-40444	Remote Code Execution	Important	Yes	Yes	0
			CVE-2021-38635	Information Disclosure	Important	No	No	2
			CVE-2021-38636	Information Disclosure	Important	No	No	2
			CVE-2021-36974	Elevation of Privilege	Important	No	No	2
			CVE-2021-36959	Spoofing	Important	No	No	2
			CVE-2021-38637	Information Disclosure	Important	No	No	2
			CVE-2021-40447	Elevation of Privilege	Important	No	No	2
			CVE-2021-38671	Elevation of Privilege	Important	No	No	1
			CVE-2021-38632	Security Feature Bypass	Important	No	No	2
			CVE-2021-38624	Security Feature Bypass	Important	No	No	2
5005573	高危	September 14, 2021—KB5005573 (OS Build 14393.4651) for Windows 10,	CVE-2021-36958	Remote Code Execution	Important	Yes	No	1
			CVE-2021-36969	Information Disclosure	Important	No	No	2
			CVE-2021-38633	Elevation of Privilege	Important	No	No	1
			CVE-2021-38634	Elevation of Privilege	Important	No	No	2

		version 1607, all editions ,Windows Server 2016, all editions	CVE-2021-36963	Elevation of Privilege	Important	No	No	1
			CVE-2021-38638	Elevation of Privilege	Important	No	No	2
			CVE-2021-36973	Elevation of Privilege	Important	No	No	2
			CVE-2021-36965	Remote Code Execution	Critical	No	No	2
			CVE-2021-36962	Information Disclosure	Important	No	No	2
			CVE-2021-38630	Elevation of Privilege	Important	No	No	2
			CVE-2021-36967	Elevation of Privilege	Important	No	No	2
			CVE-2021-26435	Remote Code Execution	Critical	No	No	2
			CVE-2021-36964	Elevation of Privilege	Important	No	No	2
			CVE-2021-36955	Elevation of Privilege	Important	No	No	1
			CVE-2021-38667	Elevation of Privilege	Important	No	No	2
			CVE-2021-38628	Elevation of Privilege	Important	No	No	2
			CVE-2021-36961	Denial of Service	Important	No	No	2
			CVE-2021-36960	Information Disclosure	Important	No	No	2
			CVE-2021-38639	Elevation of Privilege	Important	No	No	1
			CVE-2021-36972	Information Disclosure	Important	No	No	2

			CVE-2021-38629	Information Disclosure	Important	No	No	2
			CVE-2021-40444	Remote Code Execution	Important	Yes	Yes	0
			CVE-2021-38635	Information Disclosure	Important	No	No	2
			CVE-2021-38636	Information Disclosure	Important	No	No	2
			CVE-2021-36974	Elevation of Privilege	Important	No	No	2
			CVE-2021-36959	Spoofing	Important	No	No	2
			CVE-2021-40447	Elevation of Privilege	Important	No	No	2
			CVE-2021-38671	Elevation of Privilege	Important	No	No	1
			CVE-2021-38632	Security Feature Bypass	Important	No	No	2
			CVE-2021-38624	Security Feature Bypass	Important	No	No	2
5005607	高危	September 14, 2021—KB5005607 (Security-only update) for Windows Server 2012, Windows Embedded 8 Standard	CVE-2021-36958	Remote Code Execution	Important	Yes	No	1
			CVE-2021-36969	Information Disclosure	Important	No	No	2
			CVE-2021-38633	Elevation of Privilege	Important	No	No	1
			CVE-2021-36963	Elevation of Privilege	Important	No	No	1
			CVE-2021-38638	Elevation of Privilege	Important	No	No	2
			CVE-2021-36962	Information Disclosure	Important	No	No	2
			CVE-2021-36965	Remote Code Execution	Critical	No	No	2
			CVE-2021-26435	Remote Code	Critical	No	No	2

				Execution				
			CVE-2021-36964	Elevation of Privilege	Important	No	No	2
			CVE-2021-36955	Elevation of Privilege	Important	No	No	1
			CVE-2021-38667	Elevation of Privilege	Important	No	No	2
			CVE-2021-36959	Spoofing	Important	No	No	2
			CVE-2021-38628	Elevation of Privilege	Important	No	No	2
			CVE-2021-36961	Denial of Service	Important	No	No	2
			CVE-2021-36960	Information Disclosure	Important	No	No	2
			CVE-2021-38639	Elevation of Privilege	Important	No	No	1
			CVE-2021-36972	Information Disclosure	Important	No	No	2
			CVE-2021-38635	Information Disclosure	Important	No	No	2
			CVE-2021-38636	Information Disclosure	Important	No	No	2
			CVE-2021-36974	Elevation of Privilege	Important	No	No	2
			CVE-2021-38629	Information Disclosure	Important	No	No	2
			CVE-2021-40447	Elevation of Privilege	Important	No	No	2
			CVE-2021-38671	Elevation of Privilege	Important	No	No	1
5005568	高危	September 14, 2021—KB500556	CVE-2021-36958	Remote Code Execution	Important	Yes	No	1
			CVE-2021-36966	Elevation of	Important	No	No	2

		8 (OS Build 17763.2183) for Windows 10 Enterprise 2019 LTSC,Windows 10 IoT Enterprise 2019 LTSC,Windows 10 IoT Core 2019 LTSC,Windows Server 2019		Privilege				
			CVE-2021-36969	Information Disclosure	Important	No	No	2
			CVE-2021-38633	Elevation of Privilege	Important	No	No	1
			CVE-2021-38634	Elevation of Privilege	Important	No	No	2
			CVE-2021-36963	Elevation of Privilege	Important	No	No	1
			CVE-2021-36975	Elevation of Privilege	Important	No	No	1
			CVE-2021-38638	Elevation of Privilege	Important	No	No	2
			CVE-2021-36973	Elevation of Privilege	Important	No	No	2
			CVE-2021-36965	Remote Code Execution	Critical	No	No	2
			CVE-2021-36962	Information Disclosure	Important	No	No	2
			CVE-2021-38630	Elevation of Privilege	Important	No	No	2
			CVE-2021-36967	Elevation of Privilege	Important	No	No	2
			CVE-2021-26435	Remote Code Execution	Critical	No	No	2
			CVE-2021-36964	Elevation of Privilege	Important	No	No	2
			CVE-2021-36955	Elevation of Privilege	Important	No	No	1
			CVE-2021-38667	Elevation of Privilege	Important	No	No	2

			CVE-2021-38628	Elevation of Privilege	Important	No	No	2
			CVE-2021-36961	Denial of Service	Important	No	No	2
			CVE-2021-36960	Information Disclosure	Important	No	No	2
			CVE-2021-38639	Elevation of Privilege	Important	No	No	1
			CVE-2021-36972	Information Disclosure	Important	No	No	2
			CVE-2021-38629	Information Disclosure	Important	No	No	2
			CVE-2021-36954	Elevation of Privilege	Important	No	No	2
			CVE-2021-40444	Remote Code Execution	Important	Yes	Yes	0
			CVE-2021-38635	Information Disclosure	Important	No	No	2
			CVE-2021-38636	Information Disclosure	Important	No	No	2
			CVE-2021-36974	Elevation of Privilege	Important	No	No	2
			CVE-2021-36959	Spoofing	Important	No	No	2
			CVE-2021-38637	Information Disclosure	Important	No	No	2
			CVE-2021-40447	Elevation of Privilege	Important	No	No	2
			CVE-2021-38671	Elevation of Privilege	Important	No	No	1
			CVE-2021-38632	Security Feature Bypass	Important	No	No	2
			CVE-2021-38624	Security Feature Bypass	Important	No	No	2
5005618	高危	Septembe	CVE-2021-36958	Remote Code	Important	Yes	No	1

		r 14, 2021—KB5005618 (Security-only update) for Windows Server 2008		Execution				
			CVE-2021-38633	Elevation of Privilege	Important	No	No	1
			CVE-2021-36963	Elevation of Privilege	Important	No	No	1
			CVE-2021-38626	Elevation of Privilege	Important	No	No	2
			CVE-2021-38638	Elevation of Privilege	Important	No	No	2
			CVE-2021-36965	Remote Code Execution	Critical	No	No	2
			CVE-2021-36964	Elevation of Privilege	Important	No	No	2
			CVE-2021-36955	Elevation of Privilege	Important	No	No	1
			CVE-2021-38667	Elevation of Privilege	Important	No	No	2
			CVE-2021-36959	Spoofing	Important	No	No	2
			CVE-2021-38628	Elevation of Privilege	Important	No	No	2
			CVE-2021-38625	Elevation of Privilege	Important	No	No	2
			CVE-2021-36961	Denial of Service	Important	No	No	2
			CVE-2021-36968	Elevation of Privilege	Important	Yes	No	2
			CVE-2021-38639	Elevation of Privilege	Important	No	No	1
			CVE-2021-38635	Information Disclosure	Important	No	No	2
			CVE-2021-38636	Information	Important	No	No	2

				Disclosure				
			CVE-2021-36962	Information Disclosure	Important	No	No	2
			CVE-2021-38629	Information Disclosure	Important	No	No	2
			CVE-2021-40447	Elevation of Privilege	Important	No	No	2
			CVE-2021-38671	Elevation of Privilege	Important	No	No	1

本月微软发布的软件安全更新补丁共 12 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
4484108	高危	Office 2013	CVE-2021-38650	Spoofing	Important	No	No	2
5002007	高危	Office 2013	CVE-2021-38658	Remote Code Execution	Important	No	No	2
5001997	高危	Office 2016	CVE-2021-38646	Remote Code Execution	Important	No	No	2
5002003	高危	Excel 2016	CVE-2021-38655	Remote Code Execution	Important	No	No	2
5001958	高危	Office 2013	CVE-2021-38646	Remote Code Execution	Important	No	No	2
5002009	高危	Office Web Apps Server 2013	CVE-2021-38655	Remote Code Execution	Important	No	No	2
4484103	高危	Office 2016	CVE-2021-38650	Spoofing	Important	No	No	2
5002020	高危	SharePoint Enterprise Server 2016	CVE-2021-38652	Spoofing	Important	No	No	2
			CVE-2021-38651	Spoofing	Important	No	No	2
5002024	高危	SharePoint	CVE-2021-38652	Spoofing	Important	No	No	2

		Foundation 2013	CVE-2021-38651	Spoofing	Important	No	No	2
5002014	高危	Excel 2013	CVE-2021-38655	Remote Code Execution	Important	No	No	2
			CVE-2021-38660	Remote Code Execution	Important	No	No	2
5002005	高危	Office 2016	CVE-2021-38658	Remote Code Execution	Important	No	No	2
5005563	高危	Internet Explorer	CVE-2021-40444	Remote Code Execution	Important	Yes	Yes	0

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
4484467	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