

奇安信集团 2021 年 11 月补丁库 更新通告

第一次更新



奇安信集团漏洞补丁运营团队

2021 年 11 月 10 日

目 录

第 1 章 安全通告.....	2
第 2 章 重点关注补丁.....	3
第 3 章 已知问题和特殊调整.....	5
第 4 章 漏洞补丁详细列表.....	6
第 5 章 参考链接.....	23

文档信息

文档名称	奇安信集团 2021 年 11 月补丁库更新通告		
文档编号	Qi An Xin Group-MSPatch-2021-1101		
发布日期	2021-11-10	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：2021.11.10.1）已发布，本次更新推送了 22 个微软安全补丁，修复了 35 个安全漏洞，其中 3 个微软官方评级为“严重 (Critical)”，32 个评级为“重要 (Important)”，这些漏洞影响产品 Windows、Internet Explorer 和 Microsoft Office。

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 8 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
5002056	CVE-2021-42292	Security Feature Bypass	Important	No	Yes	Exploitation Detected
4486670						
5002035						
5002072						
5007409	CVE-2021-42321	Remote Code Execution	Important	No	Yes	Exploitation Detected
5007247	CVE-2021-38666	Remote Code Execution	Critical	No	No	Exploitation More Likely
5007189						
5007255						
5007192						
5007260						
5007207						
5007263						
5007206						
5007236						
5007245						
5007233						
5007246						
5007186						
5007247						
5007189						
5007255						
5007192						
5007260						
5007207						
5007263						

5007206						
5007236						
5007245						
5007233						
5007246						
5007186						
5007247	CVE-2021-38631	Information Disclosure	Important	Yes	No	Exploitation Less Likely
5007189						
5007255						
5007192						
5007260						
5007207						
5007263						
5007206						
5007236						
5007245						
5007233						
5007246						
5007186						
5007189	CVE-2021-41356	Denial of Service	Important	No	No	Exploitation More Likely
5007192						
5007207						
5007206						
5007186						
5007189	CVE-2021-42279	Remote Code Execution	Critical	No	No	Exploitation Less Likely
5007192						
5007207						
5007206						
5007186						
5007189	CVE-2021-26443	Remote Code Execution	Critical	No	No	Exploitation Less Likely
5007206						
5007186						

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
5007247	可选的高危	November 9, 2021—KB5007247 (Monthly Rollup) for Windows 8.1, Windows Server 2012 R2, Windows Embedded 8.1 Industry Enterprise, Windows Embedded 8.1 Industry Pro	CVE-2021-42285	Elevation of Privilege	Important	No	No	2
			CVE-2021-42287	Elevation of Privilege	Important	No	No	2
			CVE-2021-42291	Elevation of Privilege	Important	No	No	2
			CVE-2021-42283	Elevation of Privilege	Important	No	No	2
			CVE-2021-42275	Remote Code Execution	Important	No	No	2
			CVE-2021-41379	Elevation of Privilege	Important	No	No	2
			CVE-2021-42282	Elevation of Privilege	Important	No	No	2
			CVE-2021-41366	Elevation of Privilege	Important	No	No	2
			CVE-2021-38665	Information Disclosure	Important	No	No	2
			CVE-2021-38666	Remote Code Execution	Critical	No	No	1
CVE-2021-41370	Elevation of	Important	No	No	2			

				Privilege				
			CVE-2021-42278	Elevation of Privilege	Important	No	No	2
			CVE-2021-42284	Denial of Service	Important	No	No	2
			CVE-2021-41371	Information Disclosure	Important	Yes	No	2
			CVE-2021-41367	Elevation of Privilege	Important	No	No	2
			CVE-2021-41377	Elevation of Privilege	Important	No	No	2
			CVE-2021-38631	Information Disclosure	Important	Yes	No	2
5007189	可选的高危	November 9, 2021—KB5007189 (OS Build 18362.1916) for Windows 10 Enterprise, version 1909, Windows 10 Enterprise and Education, version 1909, Windows 10 IoT Enterprise, version 1909	CVE-2021-41366	Elevation of Privilege	Important	No	No	2
			CVE-2021-42283	Elevation of Privilege	Important	No	No	2
			CVE-2021-42275	Remote Code Execution	Important	No	No	2
			CVE-2021-38665	Information Disclosure	Important	No	No	2
			CVE-2021-42276	Remote Code Execution	Important	No	No	2
			CVE-2021-41370	Elevation of Privilege	Important	No	No	2
			CVE-2021-41356	Denial of Service	Important	No	No	1
			CVE-2021-41371	Information Disclosure	Important	Yes	No	2
			CVE-2021-36957	Elevation of Privilege	Important	No	No	2
			CVE-2021-38666	Remote Code Execution	Critical	No	No	1
			CVE-2021-41378	Remote Code Execution	Important	No	No	2

			CVE-2021-42288	Security Feature Bypass	Important	No	No	2
			CVE-2021-41377	Elevation of Privilege	Important	No	No	2
			CVE-2021-42277	Elevation of Privilege	Important	No	No	2
			CVE-2021-42280	Elevation of Privilege	Important	No	No	2
			CVE-2021-38631	Information Disclosure	Important	Yes	No	2
			CVE-2021-42285	Elevation of Privilege	Important	No	No	2
			CVE-2021-41379	Elevation of Privilege	Important	No	No	2
			CVE-2021-41351	Spoofing	Important	No	No	2
			CVE-2021-42284	Denial of Service	Important	No	No	2
			CVE-2021-42279	Remote Code Execution	Critical	No	No	2
			CVE-2021-26443	Remote Code Execution	Critical	No	No	2
			CVE-2021-41367	Elevation of Privilege	Important	No	No	2
5007255	高危	November 9, 2021—KB5007255 (Security-only update) for Windows 8.1, Windows Server	CVE-2021-42285	Elevation of Privilege	Important	No	No	2
			CVE-2021-42287	Elevation of Privilege	Important	No	No	2
			CVE-2021-42291	Elevation of Privilege	Important	No	No	2
			CVE-2021-42283	Elevation of Privilege	Important	No	No	2

		2012 R2, Windows Embedded 8.1 Industry Enterprise, Windows Embedded 8.1 Industry Pro	CVE-2021-42275	Remote Code Execution	Important	No	No	2
			CVE-2021-41379	Elevation of Privilege	Important	No	No	2
			CVE-2021-42282	Elevation of Privilege	Important	No	No	2
			CVE-2021-41366	Elevation of Privilege	Important	No	No	2
			CVE-2021-38665	Information Disclosure	Important	No	No	2
			CVE-2021-38666	Remote Code Execution	Critical	No	No	1
			CVE-2021-41370	Elevation of Privilege	Important	No	No	2
			CVE-2021-42278	Elevation of Privilege	Important	No	No	2
			CVE-2021-42284	Denial of Service	Important	No	No	2
			CVE-2021-41371	Information Disclosure	Important	Yes	No	2
			CVE-2021-41367	Elevation of Privilege	Important	No	No	2
			CVE-2021-41377	Elevation of Privilege	Important	No	No	2
			CVE-2021-38631	Information Disclosure	Important	Yes	No	2
5007192	高危	November 9, 2021—KB5007192 (OS Build 14393.4770) for Windows 10,	CVE-2021-42287	Elevation of Privilege	Important	No	No	2
			CVE-2021-41366	Elevation of Privilege	Important	No	No	2
			CVE-2021-42283	Elevation of Privilege	Important	No	No	2

version 1607, all editions, Windows Server 2016, all editions	CVE-2021-42275	Remote Code Execution	Important	No	No	2
	CVE-2021-42282	Elevation of Privilege	Important	No	No	2
	CVE-2021-38665	Information Disclosure	Important	No	No	2
	CVE-2021-42276	Remote Code Execution	Important	No	No	2
	CVE-2021-41370	Elevation of Privilege	Important	No	No	2
	CVE-2021-42278	Elevation of Privilege	Important	No	No	2
	CVE-2021-41356	Denial of Service	Important	No	No	1
	CVE-2021-41371	Information Disclosure	Important	Yes	No	2
	CVE-2021-36957	Elevation of Privilege	Important	No	No	2
	CVE-2021-42291	Elevation of Privilege	Important	No	No	2
	CVE-2021-38666	Remote Code Execution	Critical	No	No	1
	CVE-2021-41377	Elevation of Privilege	Important	No	No	2
	CVE-2021-42277	Elevation of Privilege	Important	No	No	2
	CVE-2021-42280	Elevation of Privilege	Important	No	No	2
	CVE-2021-38631	Information Disclosure	Important	Yes	No	2
	CVE-2021-42274	Denial of Service	Important	No	No	2
	CVE-2021-42285	Elevation of	Important	No	No	2

				Privilege				
			CVE-2021-41379	Elevation of Privilege	Important	No	No	2
			CVE-2021-42284	Denial of Service	Important	No	No	2
			CVE-2021-42279	Remote Code Execution	Critical	No	No	2
			CVE-2021-41367	Elevation of Privilege	Important	No	No	2
5007260	可选的高危	November 9, 2021—KB5007260 (Monthly Rollup) for Windows Server 2012, Windows Embedded Standard 8	CVE-2021-42285	Elevation of Privilege	Important	No	No	2
			CVE-2021-42287	Elevation of Privilege	Important	No	No	2
			CVE-2021-42291	Elevation of Privilege	Important	No	No	2
			CVE-2021-42283	Elevation of Privilege	Important	No	No	2
			CVE-2021-42275	Remote Code Execution	Important	No	No	2
			CVE-2021-41379	Elevation of Privilege	Important	No	No	2
			CVE-2021-42282	Elevation of Privilege	Important	No	No	2
			CVE-2021-41366	Elevation of Privilege	Important	No	No	2
			CVE-2021-38665	Information Disclosure	Important	No	No	2
			CVE-2021-38666	Remote Code Execution	Critical	No	No	1
			CVE-2021-41370	Elevation of Privilege	Important	No	No	2
			CVE-2021-42278	Elevation	Important	No	No	2

				of Privilege				
			CVE-2021-41371	Information Disclosure	Important	Yes	No	2
			CVE-2021-41367	Elevation of Privilege	Important	No	No	2
			CVE-2021-41377	Elevation of Privilege	Important	No	No	2
			CVE-2021-38631	Information Disclosure	Important	Yes	No	2
5007207	高危	November 9, 2021—KB5007207 (OS Build 10240.19119) for Windows 10	CVE-2021-42285	Elevation of Privilege	Important	No	No	2
			CVE-2021-41366	Elevation of Privilege	Important	No	No	2
			CVE-2021-42283	Elevation of Privilege	Important	No	No	2
			CVE-2021-42275	Remote Code Execution	Important	No	No	2
			CVE-2021-41379	Elevation of Privilege	Important	No	No	2
			CVE-2021-38665	Information Disclosure	Important	No	No	2
			CVE-2021-38666	Remote Code Execution	Critical	No	No	1
			CVE-2021-41370	Elevation of Privilege	Important	No	No	2
			CVE-2021-42276	Remote Code Execution	Important	No	No	2
			CVE-2021-41356	Denial of Service	Important	No	No	1
			CVE-2021-42284	Denial of Service	Important	No	No	2
			CVE-2021-42279	Remote Code Execution	Critical	No	No	2
			CVE-2021-41371	Information Disclosure	Important	Yes	No	2

				Disclosure				
			CVE-2021-41367	Elevation of Privilege	Important	No	No	2
			CVE-2021-41377	Elevation of Privilege	Important	No	No	2
			CVE-2021-42277	Elevation of Privilege	Important	No	No	2
			CVE-2021-38631	Information Disclosure	Important	Yes	No	2
5007263	高危	November 9, 2021—KB5007263 (Monthly Rollup) for Windows Server 2008 Service Pack 2	CVE-2021-42287	Elevation of Privilege	Important	No	No	2
			CVE-2021-42291	Elevation of Privilege	Important	No	No	2
			CVE-2021-42283	Elevation of Privilege	Important	No	No	2
			CVE-2021-42275	Remote Code Execution	Important	No	No	2
			CVE-2021-41379	Elevation of Privilege	Important	No	No	2
			CVE-2021-42282	Elevation of Privilege	Important	No	No	2
			CVE-2021-38666	Remote Code Execution	Critical	No	No	1
			CVE-2021-41370	Elevation of Privilege	Important	No	No	2
			CVE-2021-42278	Elevation of Privilege	Important	No	No	2
			CVE-2021-41371	Information Disclosure	Important	Yes	No	2
			CVE-2021-41367	Elevation of Privilege	Important	No	No	2

			CVE-2021-41377	Elevation of Privilege	Important	No	No	2
			CVE-2021-38631	Information Disclosure	Important	Yes	No	2
5007206	可选的高危	November 9, 2021—KB5007206 (OS Build 17763.2300) for Windows 10 Enterprise 2019 LTSC, Windows 10 IoT Enterprise 2019 LTSC, Windows 10 IoT Core 2019 LTSC	CVE-2021-42287	Elevation of Privilege	Important	No	No	2
			CVE-2021-41366	Elevation of Privilege	Important	No	No	2
			CVE-2021-42283	Elevation of Privilege	Important	No	No	2
			CVE-2021-42275	Remote Code Execution	Important	No	No	2
			CVE-2021-42282	Elevation of Privilege	Important	No	No	2
			CVE-2021-38665	Information Disclosure	Important	No	No	2
			CVE-2021-42276	Remote Code Execution	Important	No	No	2
			CVE-2021-41370	Elevation of Privilege	Important	No	No	2
			CVE-2021-42278	Elevation of Privilege	Important	No	No	2
			CVE-2021-41356	Denial of Service	Important	No	No	1
			CVE-2021-41371	Information Disclosure	Important	Yes	No	2
			CVE-2021-36957	Elevation of Privilege	Important	No	No	2
			CVE-2021-42291	Elevation of Privilege	Important	No	No	2
			CVE-2021-38666	Remote Code Execution	Critical	No	No	1
CVE-2021-41378	Remote Code Execution	Important	No	No	2			

				Execution				
			CVE-2021-42288	Security Feature Bypass	Important	No	No	2
			CVE-2021-41377	Elevation of Privilege	Important	No	No	2
			CVE-2021-42277	Elevation of Privilege	Important	No	No	2
			CVE-2021-42280	Elevation of Privilege	Important	No	No	2
			CVE-2021-38631	Information Disclosure	Important	Yes	No	2
			CVE-2021-42274	Denial of Service	Important	No	No	2
			CVE-2021-42285	Elevation of Privilege	Important	No	No	2
			CVE-2021-41379	Elevation of Privilege	Important	No	No	2
			CVE-2021-41351	Spoofing	Important	No	No	2
			CVE-2021-42284	Denial of Service	Important	No	No	2
			CVE-2021-42279	Remote Code Execution	Critical	No	No	2
			CVE-2021-26443	Remote Code Execution	Critical	No	No	2
			CVE-2021-41367	Elevation of Privilege	Important	No	No	2
5007236	高危	November 9, 2021—KB5007236 (Monthly Rollup) for Windows 7 Enterpri	CVE-2021-42285	Elevation of Privilege	Important	No	No	2
			CVE-2021-42287	Elevation of Privilege	Important	No	No	2
			CVE-2021-42291	Elevation of Privilege	Important	No	No	2

		se ESU, Windows 7	CVE-2021-42283	Elevation of Privilege	Important	No	No	2
		Professional	CVE-2021-42275	Remote Code Execution	Important	No	No	2
		ESU, Windows 7 Ultimate	CVE-2021-41379	Elevation of Privilege	Important	No	No	2
		ESU, Windows Server 2008 R2	CVE-2021-42282	Elevation of Privilege	Important	No	No	2
		Enterprise	CVE-2021-38665	Information Disclosure	Important	No	No	2
		ESU, Windows Server 2008 R2	CVE-2021-38666	Remote Code Execution	Critical	No	No	1
		Standard	CVE-2021-41370	Elevation of Privilege	Important	No	No	2
		ESU, Windows Server 2008 R2	CVE-2021-42278	Elevation of Privilege	Important	No	No	2
		Server 2008 R2	CVE-2021-41371	Information Disclosure	Important	Yes	No	2
		Datacenter	CVE-2021-41367	Elevation of Privilege	Important	No	No	2
		ESU, Windows Embedded Standard 7	CVE-2021-41377	Elevation of Privilege	Important	No	No	2
		ESU, Windows Embedded POSReady 7 ESU	CVE-2021-38631	Information Disclosure	Important	Yes	No	2
5007245	高危	November 9, 2021—KB5007245 (Security-only update)	CVE-2021-42285	Elevation of Privilege	Important	No	No	2
			CVE-2021-42287	Elevation of Privilege	Important	No	No	2
			CVE-2021-42291	Elevation of Privilege	Important	No	No	2

		for Windows Server 2012, Windows Embedded 8 Standard		of Privilege Elevation of Privilege	Important	No	No	2
			CVE-2021-42283	Elevation of Privilege	Important	No	No	2
			CVE-2021-42275	Remote Code Execution	Important	No	No	2
			CVE-2021-41379	Elevation of Privilege	Important	No	No	2
			CVE-2021-42282	Elevation of Privilege	Important	No	No	2
			CVE-2021-41366	Elevation of Privilege	Important	No	No	2
			CVE-2021-38665	Information Disclosure	Important	No	No	2
			CVE-2021-38666	Remote Code Execution	Critical	No	No	1
			CVE-2021-41370	Elevation of Privilege	Important	No	No	2
			CVE-2021-42278	Elevation of Privilege	Important	No	No	2
			CVE-2021-41371	Information Disclosure	Important	Yes	No	2
			CVE-2021-41367	Elevation of Privilege	Important	No	No	2
			CVE-2021-41377	Elevation of Privilege	Important	No	No	2
			CVE-2021-38631	Information Disclosure	Important	Yes	No	2
5007233	高危	November 9, 2021—KB5007233 (Security-only	CVE-2021-42285	Elevation of Privilege	Important	No	No	2
			CVE-2021-42287	Elevation of Privilege	Important	No	No	2

		update) for Windows 7	CVE-2021-42291	Elevation of Privilege	Important	No	No	2
		Enterprise ESU, Windows 7	CVE-2021-42283	Elevation of Privilege	Important	No	No	2
		Professional	CVE-2021-42275	Remote Code Execution	Important	No	No	2
		ESU, Windows 7	CVE-2021-41379	Elevation of Privilege	Important	No	No	2
		Ultimate	CVE-2021-42282	Elevation of Privilege	Important	No	No	2
		ESU, Windows	CVE-2021-38665	Information Disclosure	Important	No	No	2
		Server 2008 R2	CVE-2021-38666	Remote Code Execution	Critical	No	No	1
		Enterprise ESU, Windows	CVE-2021-41370	Elevation of Privilege	Important	No	No	2
		Server 2008 R2	CVE-2021-42278	Elevation of Privilege	Important	No	No	2
		Standard ESU, Windows	CVE-2021-41371	Information Disclosure	Important	Yes	No	2
		Server 2008 R2	CVE-2021-41367	Elevation of Privilege	Important	No	No	2
		Datacenter ESU, Windows	CVE-2021-41377	Elevation of Privilege	Important	No	No	2
		Embedded Standard	CVE-2021-38631	Information Disclosure	Important	Yes	No	2
		7 ESU, Windows						
		Embedded POSReady 7 ESU						
5007246	高危	November 9, 2021— KB500724	CVE-2021-42287	Elevation of Privilege	Important	No	No	2

		6 (Security-only update) for Windows Server 2008 Service Pack 2	CVE-2021-42291	Elevation of Privilege	Important	No	No	2
			CVE-2021-42283	Elevation of Privilege	Important	No	No	2
			CVE-2021-42275	Remote Code Execution	Important	No	No	2
			CVE-2021-41379	Elevation of Privilege	Important	No	No	2
			CVE-2021-42282	Elevation of Privilege	Important	No	No	2
			CVE-2021-38666	Remote Code Execution	Critical	No	No	1
			CVE-2021-41370	Elevation of Privilege	Important	No	No	2
			CVE-2021-42278	Elevation of Privilege	Important	No	No	2
			CVE-2021-41371	Information Disclosure	Important	Yes	No	2
			CVE-2021-41367	Elevation of Privilege	Important	No	No	2
			CVE-2021-41377	Elevation of Privilege	Important	No	No	2
			CVE-2021-38631	Information Disclosure	Important	Yes	No	2
5007186	可选的高危	November 9, 2021—KB5007186 (OS Builds 19041.13 48, 19042.13 48, and 19043.13	CVE-2021-42287	Elevation of Privilege	Important	No	No	2
			CVE-2021-41366	Elevation of Privilege	Important	No	No	2
			CVE-2021-42283	Elevation of Privilege	Important	No	No	2
			CVE-2021-42275	Remote Code Execution	Important	No	No	2

48) for Windows 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		Execution				
	CVE-2021-42282	Elevation of Privilege	Important	No	No	2
	CVE-2021-38665	Information Disclosure	Important	No	No	2
	CVE-2021-42286	Elevation of Privilege	Important	No	No	2
	CVE-2021-42276	Remote Code Execution	Important	No	No	2
	CVE-2021-41370	Elevation of Privilege	Important	No	No	2
	CVE-2021-42278	Elevation of Privilege	Important	No	No	2
	CVE-2021-41356	Denial of Service	Important	No	No	1
	CVE-2021-41371	Information Disclosure	Important	Yes	No	2
	CVE-2021-36957	Elevation of Privilege	Important	No	No	2
	CVE-2021-42291	Elevation of Privilege	Important	No	No	2
	CVE-2021-38666	Remote Code Execution	Critical	No	No	1
	CVE-2021-41378	Remote Code Execution	Important	No	No	2
	CVE-2021-42288	Security Feature Bypass	Important	No	No	2
	CVE-2021-41377	Elevation of Privilege	Important	No	No	2
	CVE-2021-42277	Elevation of Privilege	Important	No	No	2
	CVE-2021-42280	Elevation of	Important	No	No	2

				Privilege				
			CVE-2021-38631	Information Disclosure	Important	Yes	No	2
			CVE-2021-42274	Denial of Service	Important	No	No	2
			CVE-2021-42285	Elevation of Privilege	Important	No	No	2
			CVE-2021-41379	Elevation of Privilege	Important	No	No	2
			CVE-2021-41351	Spoofing	Important	No	No	2
			CVE-2021-42284	Denial of Service	Important	No	No	2
			CVE-2021-42279	Remote Code Execution	Critical	No	No	2
			CVE-2021-26443	Remote Code Execution	Critical	No	No	2
			CVE-2021-41367	Elevation of Privilege	Important	No	No	2

本月微软发布的软件安全更新补丁共 9 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
5002072	高危	Excel 2013	CVE-2021-40442	Remote Code Execution	Important	No	No	2
			CVE-2021-42292	Security Feature Bypass	Important	No	Yes	0
5002032	高危	Office 2016	CVE-2021-41368	Remote Code Execution	Important	No	No	2
5002065	高危	Office Web Apps Server	CVE-2021-40442	Remote Code	Important	No	No	2

		2013		Execution				
5002035	高危	Office 2013	CVE-2021-42292	Security Feature Bypass	Important	No	Yes	0
5002063	高危	SharePoint Enterprise Server 2013	CVE-2021-40442	Remote Code Execution	Important	No	No	2
4486670	高危	Office 2016	CVE-2021-42292	Security Feature Bypass	Important	No	Yes	0
5002038	高危	Office 2013	CVE-2021-41368	Remote Code Execution	Important	No	No	2
5002056	高危	Excel 2016	CVE-2021-40442	Remote Code Execution	Important	No	No	2
			CVE-2021-42292	Security Feature Bypass	Important	No	Yes	0
5007409	高危	Exchange Server 2019	CVE-2021-42321	Remote Code Execution	Important	No	Yes	0
			CVE-2021-41349	Spoofing	Important	No	No	2
			CVE-2021-42305	Spoofing	Important	No	No	2

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>