奇安信集团 2022 年 05 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 05 月 11 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 7

第 4 章 漏洞补丁详细列表 8

第 5 章 参考链接 55

文档信息

文档名称	奇安信集团 2022 年 05 月补丁库更新通告		
文档编号	Qi An Xin Group-MSPatch-2022-0501		
发布日期	2022-05-11	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:2022.05.11.1,V10版本:2022.05.11.1000已发布，本次更新推送了 46 个微软安全补丁，修复了 68 个安全漏洞，其中 6 个微软官方评级为“严重(Critical)”，61 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 14 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
5013942	CVE-2022-22713	Denial of Service	Important	Yes	No	Exploitation Less Likely
5013963	CVE-2022-29132	Elevation of Privilege	Important	No	No	Exploitation Less Likely
5013999						
5014017						
5014001						
5013941						
5014011						
5014012						
5013952						
5014006						
5013945						
5014010						
5013943						
5014025						
5013942						
5014018						
5013963	CVE-2022-23270	Remote Code Execution	Critical	No	No	Exploitation More Likely
5013999						
5014017						
5014001						
5013941						
5014011						
5014012						
5013952						

5014006 5013945 5014010 5013943 5014025 5013942 5014018						
5013963 5013999 5014017 5014001 5013941 5014011 5014012 5013952 5014006 5013945 5014010 5013943 5014025 5013942 5014018	CVE-2022-26925	Spoofing	Important	Yes	Yes	Exploitation Detected
5013963 5014017 5014001 5013941 5014011 5013952 5013945 5013943 5014025 5013942 5014018	CVE-2022-29104	Elevation of Privilege	Important	No	No	Exploitation More Likely
5013963 5013999 5014017 5014001 5013941 5014011 5014012 5013952	CVE-2022-21972	Remote Code Execution	Critical	No	No	Exploitation Less Likely

5014006 5013945 5014010 5013943 5014025 5013942 5014018						
5013963 5014001 5013941 5014011 5013952 5013945 5013943 5014025 5013942	CVE-2022-26923	Elevation of Privilege	Critical	No	No	Exploitation More Likely
5013963 5014017 5014001 5013941 5014011 5013952 5013945 5013943 5014025 5013942 5014018	CVE-2022-29114	Information Disclosure	Important	No	No	Exploitation More Likely
5013963 5013999 5014017 5014001 5013941 5014011 5014012 5013952 5014006 5013945 5014010 5013943 5014025 5013942	CVE-2022-26931	Elevation of Privilege	Critical	No	No	Exploitation More Likely

5014018						
5002195 5002203	CVE-2022-29108	Remote Code Execution	Important	No	No	Exploitation More Likely
5013999 5014017 5014001 5013941 5014011 5014012 5013952 5014006 5014010 5013942 5014018	CVE-2022-26937	Remote Code Execution	Critical	No	No	Exploitation More Likely
5013941 5013945 5013942	CVE-2022-29142	Elevation of Privilege	Important	No	No	Exploitation More Likely
5013943	CVE-2022-22017	Remote Code Execution	Critical	No	No	Exploitation More Likely
5013942	CVE-2022-22713	Denial of Service	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 16 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
5013963	高危	May 10, 2022—KB5013963 (OS Build 10240.19297) for Windows 10	CVE-2022-22016	Elevation of Privilege	Important	No	No	2
			CVE-2022-29103	Elevation of Privilege	Important	No	No	2
			CVE-2022-22013	Remote Code Execution	Important	No	No	2
			CVE-2022-29105	Remote Code Execution	Important	No	No	2
			CVE-2022-26934	Information Disclosure	Important	No	No	2
			CVE-2022-29129	Remote Code Execution	Important	No	No	2
			CVE-2022-26930	Information Disclosure	Important	No	No	2
			CVE-2022-29139	Remote Code Execution	Important	No	No	2
			CVE-2022-26936	Information Disclosure	Important	No	No	2
			CVE-2022-26935	Information Disclosure	Important	No	No	2
			CVE-2022-29132	Elevation of Privilege	Important	No	No	1

			CVE-2022-29115	Remote Code Execution	Important	No	No	2
			CVE-2022-29112	Information Disclosure	Important	No	No	2
			CVE-2022-29126	Elevation of Privilege	Important	No	No	2
			CVE-2022-23270	Remote Code Execution	Critical	No	No	1
			CVE-2022-29141	Remote Code Execution	Important	No	No	2
			CVE-2022-26925	Spoofing	Important	Yes	Yes	0
			CVE-2022-22014	Remote Code Execution	Important	No	No	2
			CVE-2022-29125	Elevation of Privilege	Important	No	No	2
			CVE-2022-26933	Information Disclosure	Important	No	No	2
			CVE-2022-22011	Information Disclosure	Important	No	No	2
			CVE-2022-29137	Remote Code Execution	Important	No	No	2
			CVE-2022-29130	Remote Code Execution	Important	No	No	2
			CVE-2022-22019	Remote Code Execution	Important	No	No	2
			CVE-2022-22015	Information Disclosure	Important	No	No	2
			CVE-2022-29127	Security Feature Bypass	Important	No	No	2
			CVE-2022-29104	Elevation of Privilege	Important	No	No	1
			CVE-2022-21972	Remote Code Execution	Critical	No	No	2
			CVE-2022-29128	Remote Code	Important	No	No	2

				Execution				
			CVE-2022-26923	Elevation of Privilege	Critical	No	No	1
			CVE-2022-22012	Remote Code Execution	Important	No	No	2
			CVE-2022-29114	Information Disclosure	Important	No	No	1
			CVE-2022-26926	Remote Code Execution	Important	No	No	2
			CVE-2022-26931	Elevation of Privilege	Critical	No	No	2
			CVE-2022-29121	Denial of Service	Important	No	No	2
5013999	高危	May 10, 2022—KB5013999 (Security-only update) for Windows 7 Enterprise ESU, Windows 7 Professional ESU, Windows 7 Ultimate ESU, Windows Server 2008 R2 Enterprise ESU, Wind	CVE-2022-29103	Elevation of Privilege	Important	No	No	2
			CVE-2022-22013	Remote Code Execution	Important	No	No	2
			CVE-2022-29105	Remote Code Execution	Important	No	No	2
			CVE-2022-26934	Information Disclosure	Important	No	No	2
			CVE-2022-29129	Remote Code Execution	Important	No	No	2
			CVE-2022-29139	Remote Code Execution	Important	No	No	2
			CVE-2022-26936	Information Disclosure	Important	No	No	2
			CVE-2022-26935	Information Disclosure	Important	No	No	2
			CVE-2022-29132	Elevation of Privilege	Important	No	No	1
			CVE-2022-29115	Remote Code Execution	Important	No	No	2
			CVE-2022-29112	Informatio	Important	No	No	2

		ows Server 2008 R2 Standard ESU,Windows Server 2008 R2 Datacenter ESU,Windows Embedded Standard 7 ESU,Windows Embedded POSReady 7 ESU		n Disclosure				
			CVE-2022-23270	Remote Code Execution	Critical	No	No	1
			CVE-2022-29141	Remote Code Execution	Important	No	No	2
			CVE-2022-26925	Spoofing	Important	Yes	Yes	0
			CVE-2022-22014	Remote Code Execution	Important	No	No	2
			CVE-2022-26788	Elevation of Privilege	Important	No	No	2
			CVE-2022-22011	Information Disclosure	Important	No	No	2
			CVE-2022-29137	Remote Code Execution	Important	No	No	2
			CVE-2022-29130	Remote Code Execution	Important	No	No	2
			CVE-2022-26937	Remote Code Execution	Critical	No	No	1
			CVE-2022-22019	Remote Code Execution	Important	No	No	2
			CVE-2022-22015	Information Disclosure	Important	No	No	2
			CVE-2022-29127	Security Feature Bypass	Important	No	No	2
			CVE-2022-21972	Remote Code Execution	Critical	No	No	2
			CVE-2022-29128	Remote Code Execution	Important	No	No	2
			CVE-2022-22012	Remote Code Execution	Important	No	No	2
			CVE-2022-26926	Remote Code Execution	Important	No	No	2
			CVE-2022-26931	Elevation of Privilege	Critical	No	No	2
			CVE-2022-29121	Denial of Service	Important	No	No	2

5014017	高危	May 10, 2022—KB5014017 (Monthly Rollup) for Windows Server 2012, Windows Embedded 8 Standard	CVE-2022-29103	Elevation of Privilege	Important	No	No	2
			CVE-2022-22013	Remote Code Execution	Important	No	No	2
			CVE-2022-29105	Remote Code Execution	Important	No	No	2
			CVE-2022-26934	Information Disclosure	Important	No	No	2
			CVE-2022-29129	Remote Code Execution	Important	No	No	2
			CVE-2022-26930	Information Disclosure	Important	No	No	2
			CVE-2022-29139	Remote Code Execution	Important	No	No	2
			CVE-2022-29122	Information Disclosure	Important	No	No	2
			CVE-2022-26936	Information Disclosure	Important	No	No	2
			CVE-2022-29132	Elevation of Privilege	Important	No	No	1
			CVE-2022-29115	Remote Code Execution	Important	No	No	2
			CVE-2022-29112	Information Disclosure	Important	No	No	2
			CVE-2022-26935	Information Disclosure	Important	No	No	2
			CVE-2022-29120	Information Disclosure	Important	No	No	2
			CVE-2022-29126	Elevation of Privilege	Important	No	No	2
			CVE-2022-23270	Remote Code Execution	Critical	No	No	1

			CVE-2022-29141	Remote Code Execution	Important	No	No	2
			CVE-2022-26925	Spoofing	Important	Yes	Yes	0
			CVE-2022-29138	Elevation of Privilege	Important	No	No	2
			CVE-2022-22014	Remote Code Execution	Important	No	No	2
			CVE-2022-29125	Elevation of Privilege	Important	No	No	2
			CVE-2022-26933	Information Disclosure	Important	No	No	2
			CVE-2022-29151	Elevation of Privilege	Important	No	No	2
			CVE-2022-22011	Information Disclosure	Important	No	No	2
			CVE-2022-29135	Elevation of Privilege	Important	No	No	2
			CVE-2022-29130	Remote Code Execution	Important	No	No	2
			CVE-2022-29137	Remote Code Execution	Important	No	No	2
			CVE-2022-29150	Elevation of Privilege	Important	No	No	2
			CVE-2022-26937	Remote Code Execution	Critical	No	No	1
			CVE-2022-22019	Remote Code Execution	Important	No	No	2
			CVE-2022-29102	Information Disclosure	Important	No	No	2
			CVE-2022-22015	Information Disclosure	Important	No	No	2
			CVE-2022-29127	Security Feature	Important	No	No	2

				Bypass				
			CVE-2022-29104	Elevation of Privilege	Important	No	No	1
			CVE-2022-21972	Remote Code Execution	Critical	No	No	2
			CVE-2022-29128	Remote Code Execution	Important	No	No	2
			CVE-2022-29123	Information Disclosure	Important	No	No	2
			CVE-2022-22012	Remote Code Execution	Important	No	No	2
			CVE-2022-29114	Information Disclosure	Important	No	No	1
			CVE-2022-26926	Remote Code Execution	Important	No	No	2
			CVE-2022-26931	Elevation of Privilege	Critical	No	No	2
			CVE-2022-29121	Denial of Service	Important	No	No	2
5014001	高危	May 10, 2022—KB5014001 (Security-only update) for Windows 8.1, Windows RT 8.1, Windows Server 2012 R2, Windows Embedded 8.1	CVE-2022-29103	Elevation of Privilege	Important	No	No	2
			CVE-2022-22013	Remote Code Execution	Important	No	No	2
			CVE-2022-29105	Remote Code Execution	Important	No	No	2
			CVE-2022-26934	Information Disclosure	Important	No	No	2
			CVE-2022-29129	Remote Code Execution	Important	No	No	2
			CVE-2022-26930	Information Disclosure	Important	No	No	2
			CVE-2022-29139	Remote Code Execution	Important	No	No	2
			CVE-2022-29122	Information	Important	No	No	2

		Industry Enterprise,Windows Embedded 8.1 Industry Pro		Disclosure				
			CVE-2022-26936	Information Disclosure	Important	No	No	2
			CVE-2022-29132	Elevation of Privilege	Important	No	No	1
			CVE-2022-29115	Remote Code Execution	Important	No	No	2
			CVE-2022-29112	Information Disclosure	Important	No	No	2
			CVE-2022-26935	Information Disclosure	Important	No	No	2
			CVE-2022-29120	Information Disclosure	Important	No	No	2
			CVE-2022-29126	Elevation of Privilege	Important	No	No	2
			CVE-2022-23270	Remote Code Execution	Critical	No	No	1
			CVE-2022-29141	Remote Code Execution	Important	No	No	2
			CVE-2022-26925	Spoofing	Important	Yes	Yes	0
			CVE-2022-29138	Elevation of Privilege	Important	No	No	2
			CVE-2022-22014	Remote Code Execution	Important	No	No	2
			CVE-2022-29125	Elevation of Privilege	Important	No	No	2
			CVE-2022-26933	Information Disclosure	Important	No	No	2
			CVE-2022-29151	Elevation of Privilege	Important	No	No	2
			CVE-2022-22011	Information	Important	No	No	2

				Disclosure				
			CVE-2022-29135	Elevation of Privilege	Important	No	No	2
			CVE-2022-29137	Remote Code Execution	Important	No	No	2
			CVE-2022-29130	Remote Code Execution	Important	No	No	2
			CVE-2022-29150	Elevation of Privilege	Important	No	No	2
			CVE-2022-26937	Remote Code Execution	Critical	No	No	1
			CVE-2022-22019	Remote Code Execution	Important	No	No	2
			CVE-2022-29102	Information Disclosure	Important	No	No	2
			CVE-2022-22015	Information Disclosure	Important	No	No	2
			CVE-2022-29127	Security Feature Bypass	Important	No	No	2
			CVE-2022-29104	Elevation of Privilege	Important	No	No	1
			CVE-2022-21972	Remote Code Execution	Critical	No	No	2
			CVE-2022-29128	Remote Code Execution	Important	No	No	2
			CVE-2022-29123	Information Disclosure	Important	No	No	2
			CVE-2022-26923	Elevation of Privilege	Critical	No	No	1
			CVE-2022-22012	Remote Code Execution	Important	No	No	2
			CVE-2022-26926	Remote Code Execution	Important	No	No	2
			CVE-2022-29114	Information	Important	No	No	1

				n Disclosure				
			CVE-2022-29134	Information Disclosure	Important	No	No	2
			CVE-2022-26931	Elevation of Privilege	Critical	No	No	2
			CVE-2022-29121	Denial of Service	Important	No	No	2
5013941	高危	May 10, 2022—KB5013941 (OS Build 17763.2928) for Windows 10 Enterprise 2019 LTSC, Windows 10 IoT Enterprise 2019 LTSC, Windows 10 IoT Core 2019 LTSC	CVE-2022-22016	Elevation of Privilege	Important	No	No	2
			CVE-2022-29103	Elevation of Privilege	Important	No	No	2
			CVE-2022-22013	Remote Code Execution	Important	No	No	2
			CVE-2022-24466	Security Feature Bypass	Important	No	No	2
			CVE-2022-29105	Remote Code Execution	Important	No	No	2
			CVE-2022-26934	Information Disclosure	Important	No	No	2
			CVE-2022-29129	Remote Code Execution	Important	No	No	2
			CVE-2022-26930	Information Disclosure	Important	No	No	2
			CVE-2022-29139	Remote Code Execution	Important	No	No	2
			CVE-2022-29140	Information Disclosure	Important	No	No	2
			CVE-2022-29131	Remote Code Execution	Important	No	No	2
			CVE-2022-29132	Elevation of Privilege	Important	No	No	1
			CVE-2022-29122	Informatio	Important	No	No	2

				n Disclosure				
			CVE-2022-29115	Remote Code Execution	Important	No	No	2
			CVE-2022-29112	Information Disclosure	Important	No	No	2
			CVE-2022-29120	Information Disclosure	Important	No	No	2
			CVE-2022-26936	Information Disclosure	Important	No	No	2
			CVE-2022-26935	Information Disclosure	Important	No	No	2
			CVE-2022-26927	Remote Code Execution	Important	No	No	2
			CVE-2022-26939	Elevation of Privilege	Important	No	No	2
			CVE-2022-29142	Elevation of Privilege	Important	No	No	1
			CVE-2022-29126	Elevation of Privilege	Important	No	No	2
			CVE-2022-29141	Remote Code Execution	Important	No	No	2
			CVE-2022-23270	Remote Code Execution	Critical	No	No	1
			CVE-2022-26938	Elevation of Privilege	Important	No	No	2
			CVE-2022-26925	Spoofing	Important	Yes	Yes	0
			CVE-2022-26913	Security Feature Bypass	Important	No	No	2
			CVE-2022-29138	Elevation of Privilege	Important	No	No	2
			CVE-2022-22014	Remote Code	Important	No	No	2

				Execution				
			CVE-2022-29125	Elevation of Privilege	Important	No	No	2
			CVE-2022-26933	Information Disclosure	Important	No	No	2
			CVE-2022-29151	Elevation of Privilege	Important	No	No	2
			CVE-2022-22011	Information Disclosure	Important	No	No	2
			CVE-2022-29135	Elevation of Privilege	Important	No	No	2
			CVE-2022-29137	Remote Code Execution	Important	No	No	2
			CVE-2022-29130	Remote Code Execution	Important	No	No	2
			CVE-2022-29150	Elevation of Privilege	Important	No	No	2
			CVE-2022-29113	Elevation of Privilege	Important	No	No	2
			CVE-2022-26937	Remote Code Execution	Critical	No	No	1
			CVE-2022-22019	Remote Code Execution	Important	No	No	2
			CVE-2022-29102	Information Disclosure	Important	No	No	2
			CVE-2022-29106	Elevation of Privilege	Important	No	No	2
			CVE-2022-22015	Information Disclosure	Important	No	No	2
			CVE-2022-29127	Security Feature Bypass	Important	No	No	2

			CVE-2022-29104	Elevation of Privilege	Important	No	No	1
			CVE-2022-21972	Remote Code Execution	Critical	No	No	2
			CVE-2022-29128	Remote Code Execution	Important	No	No	2
			CVE-2022-29123	Information Disclosure	Important	No	No	2
			CVE-2022-26923	Elevation of Privilege	Critical	No	No	1
			CVE-2022-22012	Remote Code Execution	Important	No	No	2
			CVE-2022-26926	Remote Code Execution	Important	No	No	2
			CVE-2022-29114	Information Disclosure	Important	No	No	1
			CVE-2022-29134	Information Disclosure	Important	No	No	2
			CVE-2022-26932	Elevation of Privilege	Important	No	No	2
			CVE-2022-29121	Denial of Service	Important	No	No	2
			CVE-2022-26931	Elevation of Privilege	Critical	No	No	2
5014011	高危	May 10, 2022—KB5014011 (Monthly Rollup) for Windows 8.1, Windows RT 8.1, Wind	CVE-2022-29103	Elevation of Privilege	Important	No	No	2
			CVE-2022-22013	Remote Code Execution	Important	No	No	2
			CVE-2022-29105	Remote Code Execution	Important	No	No	2
			CVE-2022-26934	Information Disclosure	Important	No	No	2
			CVE-2022-29129	Remote Code	Important	No	No	2

		ows Server 2012 R2,Windows Embedded 8.1 Industry Enterprise,Windows Embedded 8.1 Industry Pro		Execution				
			CVE-2022-26930	Information Disclosure	Important	No	No	2
			CVE-2022-29139	Remote Code Execution	Important	No	No	2
			CVE-2022-29122	Information Disclosure	Important	No	No	2
			CVE-2022-26936	Information Disclosure	Important	No	No	2
			CVE-2022-29132	Elevation of Privilege	Important	No	No	1
			CVE-2022-29115	Remote Code Execution	Important	No	No	2
			CVE-2022-29112	Information Disclosure	Important	No	No	2
			CVE-2022-26935	Information Disclosure	Important	No	No	2
			CVE-2022-29120	Information Disclosure	Important	No	No	2
			CVE-2022-29126	Elevation of Privilege	Important	No	No	2
			CVE-2022-23270	Remote Code Execution	Critical	No	No	1
			CVE-2022-29141	Remote Code Execution	Important	No	No	2
			CVE-2022-26925	Spoofing	Important	Yes	Yes	0
			CVE-2022-29138	Elevation of Privilege	Important	No	No	2
			CVE-2022-22014	Remote Code Execution	Important	No	No	2
			CVE-2022-29125	Elevation of Privilege	Important	No	No	2

			CVE-2022-26933	Information Disclosure	Important	No	No	2
			CVE-2022-29151	Elevation of Privilege	Important	No	No	2
			CVE-2022-22011	Information Disclosure	Important	No	No	2
			CVE-2022-29135	Elevation of Privilege	Important	No	No	2
			CVE-2022-29137	Remote Code Execution	Important	No	No	2
			CVE-2022-29130	Remote Code Execution	Important	No	No	2
			CVE-2022-29150	Elevation of Privilege	Important	No	No	2
			CVE-2022-26937	Remote Code Execution	Critical	No	No	1
			CVE-2022-22019	Remote Code Execution	Important	No	No	2
			CVE-2022-29102	Information Disclosure	Important	No	No	2
			CVE-2022-22015	Information Disclosure	Important	No	No	2
			CVE-2022-29127	Security Feature Bypass	Important	No	No	2
			CVE-2022-29104	Elevation of Privilege	Important	No	No	1
			CVE-2022-21972	Remote Code Execution	Critical	No	No	2
			CVE-2022-29128	Remote Code Execution	Important	No	No	2
			CVE-2022-29123	Information Disclosure	Important	No	No	2

			CVE-2022-26923	Elevation of Privilege	Critical	No	No	1
			CVE-2022-22012	Remote Code Execution	Important	No	No	2
			CVE-2022-26926	Remote Code Execution	Important	No	No	2
			CVE-2022-29114	Information Disclosure	Important	No	No	1
			CVE-2022-29134	Information Disclosure	Important	No	No	2
			CVE-2022-26931	Elevation of Privilege	Critical	No	No	2
			CVE-2022-29121	Denial of Service	Important	No	No	2
5014012	高危	May 10, 2022—KB5014012 (Monthly Rollup) for Windows 7 Enterprise ESU,Windows 7 Professional ESU,Windows 7 Ultimate ESU,Windows Server 2008 R2 Enterprise	CVE-2022-29103	Elevation of Privilege	Important	No	No	2
			CVE-2022-22013	Remote Code Execution	Important	No	No	2
			CVE-2022-29105	Remote Code Execution	Important	No	No	2
			CVE-2022-26934	Information Disclosure	Important	No	No	2
			CVE-2022-29129	Remote Code Execution	Important	No	No	2
			CVE-2022-29139	Remote Code Execution	Important	No	No	2
			CVE-2022-26936	Information Disclosure	Important	No	No	2
			CVE-2022-26935	Information Disclosure	Important	No	No	2
			CVE-2022-29132	Elevation of Privilege	Important	No	No	1
			CVE-2022-29115	Remote Code	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		Execution				
			CVE-2022-29112	Information Disclosure	Important	No	No	2
			CVE-2022-23270	Remote Code Execution	Critical	No	No	1
			CVE-2022-29141	Remote Code Execution	Important	No	No	2
			CVE-2022-26925	Spoofing	Important	Yes	Yes	0
			CVE-2022-22014	Remote Code Execution	Important	No	No	2
			CVE-2022-26788	Elevation of Privilege	Important	No	No	2
			CVE-2022-22011	Information Disclosure	Important	No	No	2
			CVE-2022-29137	Remote Code Execution	Important	No	No	2
			CVE-2022-29130	Remote Code Execution	Important	No	No	2
			CVE-2022-26937	Remote Code Execution	Critical	No	No	1
			CVE-2022-22019	Remote Code Execution	Important	No	No	2
			CVE-2022-22015	Information Disclosure	Important	No	No	2
			CVE-2022-29127	Security Feature Bypass	Important	No	No	2
			CVE-2022-21972	Remote Code Execution	Critical	No	No	2
			CVE-2022-29128	Remote Code Execution	Important	No	No	2
			CVE-2022-22012	Remote Code Execution	Important	No	No	2
			CVE-2022-26926	Remote Code Execution	Important	No	No	2
			CVE-2022-26931	Elevation of Privilege	Critical	No	No	2

			CVE-2022-29121	Denial of Service	Important	No	No	2
5013952	高危	May 10, 2022—KB5013952 (OS Build 14393.5125) for Windows 10, version 1607, all editions ,Windows Server 2016, all editions	CVE-2022-22016	Elevation of Privilege	Important	No	No	2
			CVE-2022-29103	Elevation of Privilege	Important	No	No	2
			CVE-2022-22013	Remote Code Execution	Important	No	No	2
			CVE-2022-24466	Security Feature Bypass	Important	No	No	2
			CVE-2022-29105	Remote Code Execution	Important	No	No	2
			CVE-2022-26934	Information Disclosure	Important	No	No	2
			CVE-2022-29129	Remote Code Execution	Important	No	No	2
			CVE-2022-26930	Information Disclosure	Important	No	No	2
			CVE-2022-29139	Remote Code Execution	Important	No	No	2
			CVE-2022-29140	Information Disclosure	Important	No	No	2
			CVE-2022-29122	Information Disclosure	Important	No	No	2
			CVE-2022-29132	Elevation of Privilege	Important	No	No	1
			CVE-2022-29115	Remote Code Execution	Important	No	No	2
			CVE-2022-29112	Information Disclosure	Important	No	No	2
			CVE-2022-26936	Information Disclosure	Important	No	No	2

			CVE-2022-29120	Information Disclosure	Important	No	No	2
			CVE-2022-26935	Information Disclosure	Important	No	No	2
			CVE-2022-26939	Elevation of Privilege	Important	No	No	2
			CVE-2022-29126	Elevation of Privilege	Important	No	No	2
			CVE-2022-23270	Remote Code Execution	Critical	No	No	1
			CVE-2022-29141	Remote Code Execution	Important	No	No	2
			CVE-2022-26938	Elevation of Privilege	Important	No	No	2
			CVE-2022-26925	Spoofing	Important	Yes	Yes	0
			CVE-2022-29138	Elevation of Privilege	Important	No	No	2
			CVE-2022-22014	Remote Code Execution	Important	No	No	2
			CVE-2022-29125	Elevation of Privilege	Important	No	No	2
			CVE-2022-26933	Information Disclosure	Important	No	No	2
			CVE-2022-30130	Denial of Service	Low	No	No	4
			CVE-2022-29151	Elevation of Privilege	Important	No	No	2
			CVE-2022-22011	Information Disclosure	Important	No	No	2
			CVE-2022-29135	Elevation of Privilege	Important	No	No	2

			CVE-2022-29137	Remote Code Execution	Important	No	No	2
			CVE-2022-29130	Remote Code Execution	Important	No	No	2
			CVE-2022-29150	Elevation of Privilege	Important	No	No	2
			CVE-2022-26937	Remote Code Execution	Critical	No	No	1
			CVE-2022-22019	Remote Code Execution	Important	No	No	2
			CVE-2022-29102	Information Disclosure	Important	No	No	2
			CVE-2022-29106	Elevation of Privilege	Important	No	No	2
			CVE-2022-22015	Information Disclosure	Important	No	No	2
			CVE-2022-29127	Security Feature Bypass	Important	No	No	2
			CVE-2022-29104	Elevation of Privilege	Important	No	No	1
			CVE-2022-21972	Remote Code Execution	Critical	No	No	2
			CVE-2022-29128	Remote Code Execution	Important	No	No	2
			CVE-2022-29123	Information Disclosure	Important	No	No	2
			CVE-2022-26923	Elevation of Privilege	Critical	No	No	1
			CVE-2022-22012	Remote Code Execution	Important	No	No	2
			CVE-2022-26926	Remote Code Execution	Important	No	No	2
			CVE-2022-29114	Information	Important	No	No	1

				Disclosure				
			CVE-2022-29134	Information Disclosure	Important	No	No	2
			CVE-2022-26932	Elevation of Privilege	Important	No	No	2
			CVE-2022-29121	Denial of Service	Important	No	No	2
			CVE-2022-26931	Elevation of Privilege	Critical	No	No	2
5014006	高危	May 10, 2022—KB5014006 (Security-only update) for Windows Server 2008 Service Pack 2	CVE-2022-29103	Elevation of Privilege	Important	No	No	2
			CVE-2022-22013	Remote Code Execution	Important	No	No	2
			CVE-2022-26934	Information Disclosure	Important	No	No	2
			CVE-2022-29129	Remote Code Execution	Important	No	No	2
			CVE-2022-29139	Remote Code Execution	Important	No	No	2
			CVE-2022-26936	Information Disclosure	Important	No	No	2
			CVE-2022-26935	Information Disclosure	Important	No	No	2
			CVE-2022-29132	Elevation of Privilege	Important	No	No	1
			CVE-2022-29115	Remote Code Execution	Important	No	No	2
			CVE-2022-29112	Information Disclosure	Important	No	No	2
			CVE-2022-23270	Remote Code Execution	Critical	No	No	1
			CVE-2022-29141	Remote Code Execution	Important	No	No	2

			CVE-2022-26925	Spoofing	Important	Yes	Yes	0
			CVE-2022-22014	Remote Code Execution	Important	No	No	2
			CVE-2022-22011	Information Disclosure	Important	No	No	2
			CVE-2022-29130	Remote Code Execution	Important	No	No	2
			CVE-2022-29137	Remote Code Execution	Important	No	No	2
			CVE-2022-26937	Remote Code Execution	Critical	No	No	1
			CVE-2022-22019	Remote Code Execution	Important	No	No	2
			CVE-2022-29127	Security Feature Bypass	Important	No	No	2
			CVE-2022-21972	Remote Code Execution	Critical	No	No	2
			CVE-2022-29128	Remote Code Execution	Important	No	No	2
			CVE-2022-22012	Remote Code Execution	Important	No	No	2
			CVE-2022-26926	Remote Code Execution	Important	No	No	2
			CVE-2022-26931	Elevation of Privilege	Critical	No	No	2
			CVE-2022-29121	Denial of Service	Important	No	No	2
5013945	高危	May 10, 2022—KB5013945 (OS Build 18363.2274) for Windows 10 Enterprise, version	CVE-2022-22016	Elevation of Privilege	Important	No	No	2
			CVE-2022-29103	Elevation of Privilege	Important	No	No	2
			CVE-2022-22013	Remote Code Execution	Important	No	No	2
			CVE-2022-24466	Security Feature Bypass	Important	No	No	2
			CVE-2022-29105	Remote Code	Important	No	No	2

		1909,Windows 10 Enterprise and Education, version 1909		Execution				
			CVE-2022-26934	Information Disclosure	Important	No	No	2
			CVE-2022-29129	Remote Code Execution	Important	No	No	2
			CVE-2022-26930	Information Disclosure	Important	No	No	2
			CVE-2022-29139	Remote Code Execution	Important	No	No	2
			CVE-2022-29140	Information Disclosure	Important	No	No	2
			CVE-2022-29131	Remote Code Execution	Important	No	No	2
			CVE-2022-29132	Elevation of Privilege	Important	No	No	1
			CVE-2022-29115	Remote Code Execution	Important	No	No	2
			CVE-2022-29112	Information Disclosure	Important	No	No	2
			CVE-2022-26936	Information Disclosure	Important	No	No	2
			CVE-2022-26935	Information Disclosure	Important	No	No	2
			CVE-2022-26927	Remote Code Execution	Important	No	No	2
			CVE-2022-29142	Elevation of Privilege	Important	No	No	1
			CVE-2022-29126	Elevation of Privilege	Important	No	No	2
			CVE-2022-29141	Remote Code Execution	Important	No	No	2
			CVE-2022-23270	Remote Code Execution	Critical	No	No	1

			CVE-2022-26925	Spoofing	Important	Yes	Yes	0
			CVE-2022-26913	Security Feature Bypass	Important	No	No	2
			CVE-2022-22014	Remote Code Execution	Important	No	No	2
			CVE-2022-29125	Elevation of Privilege	Important	No	No	2
			CVE-2022-26933	Information Disclosure	Important	No	No	2
			CVE-2022-22011	Information Disclosure	Important	No	No	2
			CVE-2022-29137	Remote Code Execution	Important	No	No	2
			CVE-2022-29130	Remote Code Execution	Important	No	No	2
			CVE-2022-29113	Elevation of Privilege	Important	No	No	2
			CVE-2022-22019	Remote Code Execution	Important	No	No	2
			CVE-2022-22015	Information Disclosure	Important	No	No	2
			CVE-2022-29127	Security Feature Bypass	Important	No	No	2
			CVE-2022-29104	Elevation of Privilege	Important	No	No	1
			CVE-2022-21972	Remote Code Execution	Critical	No	No	2
			CVE-2022-29128	Remote Code Execution	Important	No	No	2
			CVE-2022-26923	Elevation of Privilege	Critical	No	No	1
			CVE-2022-23279	Elevation of	Important	No	No	1

				Privilege				
			CVE-2022-22012	Remote Code Execution	Important	No	No	2
			CVE-2022-29114	Information Disclosure	Important	No	No	1
			CVE-2022-26926	Remote Code Execution	Important	No	No	2
			CVE-2022-26931	Elevation of Privilege	Critical	No	No	2
			CVE-2022-29121	Denial of Service	Important	No	No	2
5014010	高危	May 10, 2022—KB5014010 (Monthly Rollup) for Windows Server 2008 Service Pack 2	CVE-2022-29103	Elevation of Privilege	Important	No	No	2
			CVE-2022-22013	Remote Code Execution	Important	No	No	2
			CVE-2022-26934	Information Disclosure	Important	No	No	2
			CVE-2022-29129	Remote Code Execution	Important	No	No	2
			CVE-2022-29139	Remote Code Execution	Important	No	No	2
			CVE-2022-26936	Information Disclosure	Important	No	No	2
			CVE-2022-26935	Information Disclosure	Important	No	No	2
			CVE-2022-29132	Elevation of Privilege	Important	No	No	1
			CVE-2022-29115	Remote Code Execution	Important	No	No	2
			CVE-2022-29112	Information Disclosure	Important	No	No	2
			CVE-2022-23270	Remote Code Execution	Critical	No	No	1
			CVE-2022-29141	Remote Code	Important	No	No	2

				Execution				
			CVE-2022-26925	Spoofing	Important	Yes	Yes	0
			CVE-2022-22014	Remote Code Execution	Important	No	No	2
			CVE-2022-22011	Information Disclosure	Important	No	No	2
			CVE-2022-29130	Remote Code Execution	Important	No	No	2
			CVE-2022-29137	Remote Code Execution	Important	No	No	2
			CVE-2022-26937	Remote Code Execution	Critical	No	No	1
			CVE-2022-22019	Remote Code Execution	Important	No	No	2
			CVE-2022-29127	Security Feature Bypass	Important	No	No	2
			CVE-2022-21972	Remote Code Execution	Critical	No	No	2
			CVE-2022-29128	Remote Code Execution	Important	No	No	2
			CVE-2022-22012	Remote Code Execution	Important	No	No	2
			CVE-2022-26926	Remote Code Execution	Important	No	No	2
			CVE-2022-26931	Elevation of Privilege	Critical	No	No	2
			CVE-2022-29121	Denial of Service	Important	No	No	2
5013943	高危	May 10, 2022—KB5013943 (OS Build 22000.675) for Windows 11	CVE-2022-22016	Elevation of Privilege	Important	No	No	2
			CVE-2022-29103	Elevation of Privilege	Important	No	No	2
			CVE-2022-22013	Remote Code Execution	Important	No	No	2
			CVE-2022-24466	Security Feature Bypass	Important	No	No	2

			CVE-2022-26934	Information Disclosure	Important	No	No	2
			CVE-2022-29129	Remote Code Execution	Important	No	No	2
			CVE-2022-26930	Information Disclosure	Important	No	No	2
			CVE-2022-29139	Remote Code Execution	Important	No	No	2
			CVE-2022-29140	Information Disclosure	Important	No	No	2
			CVE-2022-29131	Remote Code Execution	Important	No	No	2
			CVE-2022-29132	Elevation of Privilege	Important	No	No	1
			CVE-2022-29115	Remote Code Execution	Important	No	No	2
			CVE-2022-29112	Information Disclosure	Important	No	No	2
			CVE-2022-26936	Information Disclosure	Important	No	No	2
			CVE-2022-26935	Information Disclosure	Important	No	No	2
			CVE-2022-26927	Remote Code Execution	Important	No	No	2
			CVE-2022-29126	Elevation of Privilege	Important	No	No	2
			CVE-2022-23270	Remote Code Execution	Critical	No	No	1
			CVE-2022-29141	Remote Code Execution	Important	No	No	2
			CVE-2022-22017	Remote Code Execution	Critical	No	No	1
			CVE-2022-26925	Spoofing	Important	Yes	Yes	0
			CVE-2022-26913	Security	Important	No	No	2

				Feature Bypass				
			CVE-2022-22014	Remote Code Execution	Important	No	No	2
			CVE-2022-29125	Elevation of Privilege	Important	No	No	2
			CVE-2022-26933	Information Disclosure	Important	No	No	2
			CVE-2022-26940	Information Disclosure	Important	No	No	2
			CVE-2022-29137	Remote Code Execution	Important	No	No	2
			CVE-2022-29130	Remote Code Execution	Important	No	No	2
			CVE-2022-29113	Elevation of Privilege	Important	No	No	2
			CVE-2022-29116	Information Disclosure	Important	No	No	2
			CVE-2022-22019	Remote Code Execution	Important	No	No	2
			CVE-2022-22015	Information Disclosure	Important	No	No	2
			CVE-2022-29127	Security Feature Bypass	Important	No	No	2
			CVE-2022-29104	Elevation of Privilege	Important	No	No	1
			CVE-2022-21972	Remote Code Execution	Critical	No	No	2
			CVE-2022-29128	Remote Code Execution	Important	No	No	2
			CVE-2022-29133	Elevation of Privilege	Important	No	No	2
			CVE-2022-26923	Elevation	Critical	No	No	1

				of Privilege				
			CVE-2022-23279	Elevation of Privilege	Important	No	No	1
			CVE-2022-22012	Remote Code Execution	Important	No	No	2
			CVE-2022-29114	Information Disclosure	Important	No	No	1
			CVE-2022-26926	Remote Code Execution	Important	No	No	2
			CVE-2022-26931	Elevation of Privilege	Critical	No	No	2
			CVE-2022-29121	Denial of Service	Important	No	No	2
5014025	高危	KB5014025: Servicing stack update for Windows 8.1, RT 8.1, and Server 2012 R2: May 10, 2022	CVE-2022-29103	Elevation of Privilege	Important	No	No	2
			CVE-2022-22013	Remote Code Execution	Important	No	No	2
			CVE-2022-29105	Remote Code Execution	Important	No	No	2
			CVE-2022-26934	Information Disclosure	Important	No	No	2
			CVE-2022-29129	Remote Code Execution	Important	No	No	2
			CVE-2022-26930	Information Disclosure	Important	No	No	2
			CVE-2022-29139	Remote Code Execution	Important	No	No	2
			CVE-2022-26936	Information Disclosure	Important	No	No	2
			CVE-2022-26935	Information Disclosure	Important	No	No	2
			CVE-2022-29132	Elevation of	Important	No	No	1

				Privilege				
			CVE-2022-29115	Remote Code Execution	Important	No	No	2
			CVE-2022-29112	Information Disclosure	Important	No	No	2
			CVE-2022-29126	Elevation of Privilege	Important	No	No	2
			CVE-2022-23270	Remote Code Execution	Critical	No	No	1
			CVE-2022-29141	Remote Code Execution	Important	No	No	2
			CVE-2022-26925	Spoofing	Important	Yes	Yes	0
			CVE-2022-22014	Remote Code Execution	Important	No	No	2
			CVE-2022-26933	Information Disclosure	Important	No	No	2
			CVE-2022-22011	Information Disclosure	Important	No	No	2
			CVE-2022-29137	Remote Code Execution	Important	No	No	2
			CVE-2022-29130	Remote Code Execution	Important	No	No	2
			CVE-2022-22019	Remote Code Execution	Important	No	No	2
			CVE-2022-22015	Information Disclosure	Important	No	No	2
			CVE-2022-29127	Security Feature Bypass	Important	No	No	2
			CVE-2022-29104	Elevation of Privilege	Important	No	No	1
			CVE-2022-21972	Remote Code Execution	Critical	No	No	2
			CVE-2022-29128	Remote Code Execution	Important	No	No	2
			CVE-2022-26923	Elevation	Critical	No	No	1

				of Privilege				
			CVE-2022-22012	Remote Code Execution	Important	No	No	2
			CVE-2022-29114	Information Disclosure	Important	No	No	1
			CVE-2022-26926	Remote Code Execution	Important	No	No	2
			CVE-2022-26931	Elevation of Privilege	Critical	No	No	2
			CVE-2022-29121	Denial of Service	Important	No	No	2
5013942	高危	May 10, 2022—KB5013942 (OS Builds 19042.1706, 19043.1706, and 19044.1706) for Windows 10, version 20H2, all editions, Windows Server, version 20H2, all editions, Windows 10, version 21H1, all	CVE-2022-22016	Elevation of Privilege	Important	No	No	2
			CVE-2022-29103	Elevation of Privilege	Important	No	No	2
			CVE-2022-22013	Remote Code Execution	Important	No	No	2
			CVE-2022-24466	Security Feature Bypass	Important	No	No	2
			CVE-2022-29105	Remote Code Execution	Important	No	No	2
			CVE-2022-26934	Information Disclosure	Important	No	No	2
			CVE-2022-29129	Remote Code Execution	Important	No	No	2
			CVE-2022-26930	Information Disclosure	Important	No	No	2
			CVE-2022-29139	Remote Code Execution	Important	No	No	2
			CVE-2022-29140	Information Disclosure	Important	No	No	2
			CVE-2022-29131	Remote Code Execution	Important	No	No	2

		editions ,Windows 10, version 21H2, all editions	CVE-2022-29132	Elevation of Privilege	Important	No	No	1
			CVE-2022-29122	Information Disclosure	Important	No	No	2
			CVE-2022-29115	Remote Code Execution	Important	No	No	2
			CVE-2022-29112	Information Disclosure	Important	No	No	2
			CVE-2022-29120	Information Disclosure	Important	No	No	2
			CVE-2022-26936	Information Disclosure	Important	No	No	2
			CVE-2022-26935	Information Disclosure	Important	No	No	2
			CVE-2022-26927	Remote Code Execution	Important	No	No	2
			CVE-2022-26939	Elevation of Privilege	Important	No	No	2
			CVE-2022-29142	Elevation of Privilege	Important	No	No	1
			CVE-2022-29126	Elevation of Privilege	Important	No	No	2
			CVE-2022-29141	Remote Code Execution	Important	No	No	2
			CVE-2022-23270	Remote Code Execution	Critical	No	No	1
			CVE-2022-26938	Elevation of Privilege	Important	No	No	2
			CVE-2022-26925	Spoofing	Important	Yes	Yes	0
			CVE-2022-26913	Security Feature Bypass	Important	No	No	2

			CVE-2022-22713	Denial of Service	Important	Yes	No	2
			CVE-2022-29138	Elevation of Privilege	Important	No	No	2
			CVE-2022-22014	Remote Code Execution	Important	No	No	2
			CVE-2022-29125	Elevation of Privilege	Important	No	No	2
			CVE-2022-26933	Information Disclosure	Important	No	No	2
			CVE-2022-29151	Elevation of Privilege	Important	No	No	2
			CVE-2022-22011	Information Disclosure	Important	No	No	2
			CVE-2022-29135	Elevation of Privilege	Important	No	No	2
			CVE-2022-29137	Remote Code Execution	Important	No	No	2
			CVE-2022-29130	Remote Code Execution	Important	No	No	2
			CVE-2022-29150	Elevation of Privilege	Important	No	No	2
			CVE-2022-29113	Elevation of Privilege	Important	No	No	2
			CVE-2022-26937	Remote Code Execution	Critical	No	No	1
			CVE-2022-22019	Remote Code Execution	Important	No	No	2
			CVE-2022-29102	Information Disclosure	Important	No	No	2
			CVE-2022-29106	Elevation of Privilege	Important	No	No	2

			CVE-2022-22015	Information Disclosure	Important	No	No	2
			CVE-2022-29127	Security Feature Bypass	Important	No	No	2
			CVE-2022-29104	Elevation of Privilege	Important	No	No	1
			CVE-2022-21972	Remote Code Execution	Critical	No	No	2
			CVE-2022-29128	Remote Code Execution	Important	No	No	2
			CVE-2022-29123	Information Disclosure	Important	No	No	2
			CVE-2022-26923	Elevation of Privilege	Critical	No	No	1
			CVE-2022-23279	Elevation of Privilege	Important	No	No	1
			CVE-2022-22012	Remote Code Execution	Important	No	No	2
			CVE-2022-26926	Remote Code Execution	Important	No	No	2
			CVE-2022-29114	Information Disclosure	Important	No	No	1
			CVE-2022-29134	Information Disclosure	Important	No	No	2
			CVE-2022-26932	Elevation of Privilege	Important	No	No	2
			CVE-2022-29121	Denial of Service	Important	No	No	2
			CVE-2022-26931	Elevation of Privilege	Critical	No	No	2
5014018	高危	May 10, 2022—	CVE-2022-29103	Elevation of	Important	No	No	2

		KB5014018 (Security-only update) for Windows Server 2012,Windows Embedded 8 Standard		Privilege				
			CVE-2022-22013	Remote Code Execution	Important	No	No	2
			CVE-2022-29105	Remote Code Execution	Important	No	No	2
			CVE-2022-26934	Information Disclosure	Important	No	No	2
			CVE-2022-29129	Remote Code Execution	Important	No	No	2
			CVE-2022-26930	Information Disclosure	Important	No	No	2
			CVE-2022-29139	Remote Code Execution	Important	No	No	2
			CVE-2022-29122	Information Disclosure	Important	No	No	2
			CVE-2022-26936	Information Disclosure	Important	No	No	2
			CVE-2022-29132	Elevation of Privilege	Important	No	No	1
			CVE-2022-29115	Remote Code Execution	Important	No	No	2
			CVE-2022-29112	Information Disclosure	Important	No	No	2
			CVE-2022-26935	Information Disclosure	Important	No	No	2
			CVE-2022-29120	Information Disclosure	Important	No	No	2
			CVE-2022-29126	Elevation of Privilege	Important	No	No	2
			CVE-2022-23270	Remote Code Execution	Critical	No	No	1
			CVE-2022-29141	Remote Code Execution	Important	No	No	2

			CVE-2022-26925	Spoofing	Important	Yes	Yes	0
			CVE-2022-29138	Elevation of Privilege	Important	No	No	2
			CVE-2022-22014	Remote Code Execution	Important	No	No	2
			CVE-2022-29125	Elevation of Privilege	Important	No	No	2
			CVE-2022-26933	Information Disclosure	Important	No	No	2
			CVE-2022-29151	Elevation of Privilege	Important	No	No	2
			CVE-2022-22011	Information Disclosure	Important	No	No	2
			CVE-2022-29135	Elevation of Privilege	Important	No	No	2
			CVE-2022-29130	Remote Code Execution	Important	No	No	2
			CVE-2022-29137	Remote Code Execution	Important	No	No	2
			CVE-2022-29150	Elevation of Privilege	Important	No	No	2
			CVE-2022-26937	Remote Code Execution	Critical	No	No	1
			CVE-2022-22019	Remote Code Execution	Important	No	No	2
			CVE-2022-29102	Information Disclosure	Important	No	No	2
			CVE-2022-22015	Information Disclosure	Important	No	No	2
			CVE-2022-29127	Security Feature Bypass	Important	No	No	2
			CVE-2022-29104	Elevation	Important	No	No	1

				of Privilege				
			CVE-2022-21972	Remote Code Execution	Critical	No	No	2
			CVE-2022-29128	Remote Code Execution	Important	No	No	2
			CVE-2022-29123	Information Disclosure	Important	No	No	2
			CVE-2022-22012	Remote Code Execution	Important	No	No	2
			CVE-2022-29114	Information Disclosure	Important	No	No	1
			CVE-2022-26926	Remote Code Execution	Important	No	No	2
			CVE-2022-26931	Elevation of Privilege	Critical	No	No	2
			CVE-2022-29121	Denial of Service	Important	No	No	2
5014027	高危	KB5014027: Servicing stack update for Windows Server 2012: May 10, 2022						

本月微软发布的软件安全更新补丁共 30 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
5013615	高危	May 10, 2022-Security Only Update for .NET Framework 4.8 for Windows Server 2012 (KB5013615)						
5013618	高危	May 10, 2022-Security Only Update for .NET Framework 3.5 for Windows Server 2012 (KB5013618)						
5013621	高危	May 10, 2022-Security Only Update for .NET Framework 3.5 for Windows 8.1 and Windows Server 2012 R2						

		(KB5013621)						
5013623	高危	May 10, 2022-Security Only Update for .NET Framework 4.6.2, 4.7, 4.7.1, 4.7.2 for Windows 8.1 and Windows Server 2012 R2 (KB5013623)						
5013616	高危	May 10, 2022-Security Only Update for .NET Framework 4.8 for Windows 8.1 and Windows Server 2012 R2 (KB5013616)						
5013622	高危	May 10, 2022-Security Only Update for .NET Framework 4.6.2, 4.7, 4.7.1, 4.7.2 for Windows Server 2012 (KB5013622						

		)						
5002195	高危	Description of the security update for SharePoint Enterprise Server 2016: May 10, 2022 (KB5002195)	CVE-2022-29108	Remote Code Execution	Important	No	No	1
5013837	高危	May 10, 2022-Security Only Update for .NET Framework 3.5.1, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Windows 7 SP1 and Windows Server 2008 R2 SP1 (KB5013837)	CVE-2022-30130	Denial of Service	Low	No	No	4
5013627	高危	May 10, 2022-KB5013627 Cumulative Update for .NET Framework 3.5 and 4.8 for Windows 10, version 1909	CVE-2022-30130	Denial of Service	Low	No	No	4
5013871	高危	May 10, 2022-Secur	CVE-2022-30130	Denial of Service	Low	No	No	4

		ity and Quality Rollup for .NET Framework 3.5, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Windows Server 2012 (KB5013871)						
5013839	高危	May 10, 2022-Security Only Update for .NET Framework 3.5, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Windows 8.1 and Windows Server 2012 R2 (KB5013839)	CVE-2022-30130	Denial of Service	Low	No	No	4
5013840	高危	May 10, 2022-Security Only Update for .NET Framework 2.0, 3.0, 4.6.2 for Windows Server 2008 SP2 (KB5013840)	CVE-2022-30130	Denial of Service	Low	No	No	4
5013628	高危	May 10,	CVE-2022-30130	Denial of	Low	No	No	4

		2022-KB5013628 Cumulative Update for .NET Framework 3.5 and 4.8 for Windows 11		Service				
5002187	高危	Description of the security update for Word 2013: May 10, 2022 (KB5002187)	CVE-2022-29107	Security Feature Bypass	Important	No	No	2
5013868	高危	May 10, 2022-KB5013868 Cumulative Update for .NET Framework 3.5, 4.7.2 and 4.8 for Windows 10, version 1809 and Windows Server, version 2019	CVE-2022-30130	Denial of Service	Low	No	No	4
5014260	高危	Description of the security update for Microsoft Exchange Server 2013: May	CVE-2022-21978	Elevation of Privilege	Important	No	No	2

		10, 2022 (KB5014260)						
5013873	高危	May 10, 2022-Security and Quality Rollup for .NET Framework 2.0, 3.0, 4.6.2 for Windows Server 2008 SP2 (KB5013873)	CVE-2022-30130	Denial of Service	Low	No	No	4
5013872	高危	May 10, 2022-Security and Quality Rollup for .NET Framework 3.5, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Windows 8.1, RT 8.1, and Windows Server 2012 R2 (KB5013872)	CVE-2022-30130	Denial of Service	Low	No	No	4
5002199	高危	Description of the security update for Office Web Apps Server 2013: May	CVE-2022-29110	Remote Code Execution	Important	No	No	2

		10, 2022 (KB5002199)						
5013624	高危	May 10, 2022-KB5013624 Cumulative Update for .NET Framework 3.5 and 4.8 for Windows 10, version 20H2, Windows Server, version 20H2, Windows 10 Version 21H1, and Windows 10 Version 21H2	CVE-2022-30130	Denial of Service	Low	No	No	4
4493152	高危	Description of the security update for Publisher 2016: May 10, 2022 (KB4493152)	CVE-2022-29107	Security Feature Bypass	Important	No	No	2
5013625	高危	May 10, 2022-KB5013625 Cumulative Update for .NET Framework 4.8 for Windows 10,	CVE-2022-30130	Denial of Service	Low	No	No	4

		version 1607 and Windows Server, version 2016						
5002204	高危	Description of the security update for Excel 2013: May 10, 2022 (KB5002204)	CVE-2022-29110	Remote Code Execution	Important	No	No	2
5002196	高危	Description of the security update for Excel 2016: May 10, 2022 (KB5002196)	CVE-2022-29110	Remote Code Execution	Important	No	No	2
4484347	高危	Description of the security update for Publisher 2013: May 10, 2022 (KB4484347)	CVE-2022-29107	Security Feature Bypass	Important	No	No	2
5013870	高危	May 10, 2022-Security and Quality Rollup for .NET Framework 3.5.1,	CVE-2022-30130	Denial of Service	Low	No	No	4

		4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Windows 7 SP1 and Windows Server 2008 R2 SP1 (KB5013870)						
5013838	高危	May 10, 2022-Security Only Update for .NET Framework 3.5, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Windows Server 2012 (KB5013838)	CVE-2022-30130	Denial of Service	Low	No	No	4
5002184	高危	Description of the security update for Word 2016: May 10, 2022 (KB5002184)	CVE-2022-29107	Security Feature Bypass	Important	No	No	2
5014261	高危	Description of the security update for Microsoft Exchange Server 2016 and 2019: May 10, 2022	CVE-2022-21978	Elevation of Privilege	Important	No	No	2

		(KB5014261)						
5002203	高危	Description of the security update for SharePoint Foundation 2013: May 10, 2022 (KB5002203)	CVE-2022-29108	Remote Code Execution	Important	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
5002048	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