

奇安信集团 2022 年 01 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 01 月 12 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.....	9
第 4 章 漏洞补丁详细列表.....	10
第 5 章 参考链接.....	65

文档信息

文档名称	奇安信集团 2022 年 01 月补丁库更新通告		
文档编号	Qi An Xin Group-MSPatch-2022-0101		
发布日期	2022-01-12	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:2022.01.12.1,V10 版本:2022.01.12.1000)已发布，本次更新推送了 54 个微软安全补丁，修复了 94 个安全漏洞，其中 8 个微软官方评级为“严重(Critical)”，86 个评级为“重要(Important)”，这些漏洞影响产品 Windows、Internet Explorer、.NET Framework 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 24 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
5002122	CVE-2022-21840	Remote Code Execution	Critical	No	No	Exploitation Less Likely
5002114						
4462205						
5002118						
5002064						
5002129						
5002102						
5001995						
5002060						
5002113						
5002052						
5002127						
5002124						
5002128						
5002115						
5009621	CVE-2022-21885	Elevation of Privilege	Important	No	No	Exploitation More Likely
5009566						
5009557						
5009601						
5009546						
5009627						
5009595						
5009543						
5009586						
5009545						
5009624						

5009585						
5009610						
5009619						
5009621	CVE-2022-21903	Elevation of Privilege	Important	No	No	Exploitation More Likely
5009557						
5009601						
5009546						
5009627						
5009595						
5009586						
5009545						
5009624						
5009585						
5009610						
5009619						
5009621						
5009566						
5009557						
5009601						
5009546						
5009627						
5009595						
5009543						
5009586						
5009545						
5009624						
5009585						
5009610						
5009619						
5009621	CVE-2022-21908	Elevation of Privilege	Important	No	No	Exploitation More Likely
5009566						
5009557						
5009601						
5009546						
5009627						
5009595						
5009543						
5009586						
5009545						
5009624						
5009585						
5009610						
5009619						
5009621						
5009566						
5009557						
5009601						
5009546						
5009627						
5009595						
5009543						
5009586						
5009545						
5009624						
5009585						
5009610						
5009619						
5009621	CVE-2022-21897	Elevation of Privilege	Important	No	No	Exploitation More Likely
5009566						
5009557						
5009601						
5009546						
5009627						
5009595						
5009543						
5009586						
5009545						
5009624						
5009585						
5009610						
5009619						

5009610						
5009619						
5009621	CVE-2022-21833	Elevation of Privilege	Critical	No	No	Exploitation Less Likely
5009566						
5009557						
5009601						
5009546						
5009627						
5009595						
5009543						
5009586						
5009545						
5009624						
5009585						
5009610						
5009619						
5009621	CVE-2022-21919	Elevation of Privilege	Important	Yes	No	Exploitation More Likely
5009566						
5009557						
5009601						
5009546						
5009627						
5009595						
5009543						
5009586						
5009545						
5009624						
5009585						
5009610						
5009619						
5009621	CVE-2022-21914	Elevation of Privilege	Important	No	No	Exploitation More Likely
5009566						
5009557						
5009601						
5009546						
5009627						
5009595						
5009543						
5009586						
5009545						
5009624						
5009624						

5009585						
5009610						
5009619						
5009621	CVE-2022-21836	Spoofing	Important	Yes	No	Exploitation Less Likely
5009566						
5009557						
5009601						
5009546						
5009627						
5009595						
5009543						
5009586						
5009545						
5009624						
5009585						
5009610						
5009619						
5009621	CVE-2022-21916	Elevation of Privilege	Important	No	No	Exploitation More Likely
5009566						
5009557						
5009601						
5009546						
5009627						
5009595						
5009543						
5009586						
5009545						
5009624						
5009585						
5009610						
5009619						
5009621	CVE-2022-21857	Elevation of Privilege	Critical	No	No	Exploitation Less Likely
5009566						
5009557						
5009601						
5009546						
5009627						
5009595						
5009543						
5009586						
5009545						
5009545						

5009624						
5009585						
5009610						
5009619						
5009566	CVE-2022-21907	Remote Code Execution	Critical	No	No	Exploitation More Likely
5009557						
5009543						
5009566	CVE-2022-21874	Remote Code Execution	Important	Yes	No	Exploitation Less Likely
5009557						
5009546						
5009543						
5009545						
5009585						
5009566	CVE-2021-22947	Remote Code Execution	Critical	Yes	No	Exploitation Less Likely
5009557						
5009543						
5009545						
5009566	CVE-2022-21887	Elevation of Privilege	Important	No	No	Exploitation More Likely
5009566	CVE-2022-21881	Elevation of Privilege	Important	No	No	Exploitation More Likely
5009557						
5009546						
5009595						
5009543						
5009545						
5009624						
5009585						
5009566	CVE-2022-21882	Elevation of Privilege	Important	No	No	Exploitation More Likely
5009557						
5009543						
5009545						
5009566	CVE-2021-36976	Remote Code Execution	Important	Yes	No	Exploitation Less Likely
5009557						
5009543						
5009545						
5009557	CVE-2022-21898	Remote Code Execution	Critical	No	No	Exploitation Less Likely
5009543						
5009545						
5009557	CVE-2022-21839	Denial of Service	Important	Yes	No	Exploitation Less Likely

5009557	CVE-2022-21912	Remote Code Execution	Critical	No	No	Exploitation Less Likely
5009543						
5009545						
5008631	CVE-2022-21846	Remote Code Execution	Critical	No	No	Exploitation More Likely
5008631	CVE-2022-21969	Remote Code Execution	Important	No	No	Exploitation More Likely
5008631	CVE-2022-21855	Remote Code Execution	Important	No	No	Exploitation More Likely

第3章 已知问题和特殊调整

本月暂无已知问题和特殊调整。

第4章 漏洞补丁详细列表

本月微软发布的系统安全更新补丁共 14 个，详细列表如下：

KBID	奇安信集团级别	补丁名称	CVE 编号	漏洞的影响	漏洞等级	公开披露	已受攻击	漏洞的可利用性
5009621	高危	January 11, 2022	CVE-2022-21848	Denial of Service	Important	No	No	2
		—	CVE-2022-21838	Elevation of Privilege	Important	No	No	2
		KB5009621 (Security-only update)	CVE-2022-21885	Elevation of Privilege	Important	No	No	1
		for Windows 7 Enterprise	CVE-2022-21925	Security Feature Bypass	Important	No	No	2
		ESU, Windows 7 Professional	CVE-2022-21924	Security Feature Bypass	Important	No	No	2
		ESU, Windows 7 Ultimate	CVE-2022-21903	Elevation of Privilege	Important	No	No	1
		ESU, Windows Server 2008 R2 Enterprise	CVE-2022-21908	Elevation of Privilege	Important	No	No	1
		ESU, Windows Server 2008 R2	CVE-2022-21893	Remote Code Execution	Important	No	No	2
		Enterprise	CVE-2022-21920	Elevation of Privilege	Important	No	No	2
		ESU, Windows Server 2008 R2	CVE-2022-21850	Remote Code Execution	Important	No	No	2
			CVE-2022-21922	Remote Code Execution	Important	No	No	2

		Standard ESU, Windows	CVE-2022-21905	Security Feature Bypass	Important	No	No	2
		Server 2008 R2	CVE-2022-21889	Denial of Service	Important	No	No	2
		Datacenter ESU, Windows	CVE-2022-21897	Elevation of Privilege	Important	No	No	1
		Embedded Standard 7	CVE-2022-21859	Elevation of Privilege	Important	No	No	2
		ESU, Windows	CVE-2022-21899	Security Feature Bypass	Important	No	No	2
		Embedded POSReady 7 ESU	CVE-2022-21835	Elevation of Privilege	Important	No	No	2
			CVE-2022-21880	Information Disclosure	Important	No	No	2
			CVE-2022-21833	Elevation of Privilege	Critical	No	No	2
			CVE-2022-21915	Information Disclosure	Important	No	No	2
			CVE-2022-21913	Security Feature Bypass	Important	No	No	2
			CVE-2022-21834	Elevation of Privilege	Important	No	No	2
			CVE-2022-21919	Elevation of Privilege	Important	Yes	No	1
			CVE-2022-21884	Elevation of Privilege	Important	No	No	2
			CVE-2022-21904	Information Disclosure	Important	No	No	2
			CVE-2022-21914	Elevation of Privilege	Important	No	No	1
			CVE-2022-21900	Security	Important	No	No	2

				Feature Bypass				
			CVE-2022-21883	Denial of Service	Important	No	No	2
			CVE-2022-21851	Remote Code Execution	Important	No	No	2
			CVE-2022-21890	Denial of Service	Important	No	No	2
			CVE-2022-21862	Elevation of Privilege	Important	No	No	2
			CVE-2022-21836	Spoofing	Important	Yes	No	2
			CVE-2022-21916	Elevation of Privilege	Important	No	No	1
			CVE-2022-21843	Denial of Service	Important	No	No	2
			CVE-2022-21857	Elevation of Privilege	Critical	No	No	2
5009566	高危	January 11, 2022 — KB5009566 (OS Build 22000.434) for Windows 11	CVE-2022-21959	Remote Code Execution	Important	No	No	2
			CVE-2022-21928	Remote Code Execution	Important	No	No	2
			CVE-2022-21848	Denial of Service	Important	No	No	2
			CVE-2022-21894	Security Feature Bypass	Important	No	No	2
			CVE-2022-21861	Elevation of Privilege	Important	No	No	2
			CVE-2022-21858	Elevation of Privilege	Important	No	No	2
			CVE-2022-21864	Elevation of Privilege	Important	No	No	2
			CVE-2022-21873	Elevation of Privilege	Important	No	No	2
			CVE-2022-21838	Elevation	Important	No	No	2

				of Privilege				
			CVE-2022-21907	Remote Code Execution	Critical	No	No	1
			CVE-2022-21885	Elevation of Privilege	Important	No	No	1
			CVE-2022-21962	Remote Code Execution	Important	No	No	2
			CVE-2022-21852	Elevation of Privilege	Important	No	No	2
			CVE-2022-21892	Remote Code Execution	Important	No	No	2
			CVE-2022-21925	Security Feature Bypass	Important	No	No	2
			CVE-2022-21901	Elevation of Privilege	Important	No	No	2
			CVE-2022-21924	Security Feature Bypass	Important	No	No	2
			CVE-2022-21908	Elevation of Privilege	Important	No	No	1
			CVE-2022-21877	Information Disclosure	Important	No	No	2
			CVE-2022-21893	Remote Code Execution	Important	No	No	2
			CVE-2022-21920	Elevation of Privilege	Important	No	No	2
			CVE-2022-21876	Information Disclosure	Important	No	No	2
			CVE-2022-21872	Elevation of Privilege	Important	No	No	2
			CVE-2022-21870	Elevation of Privilege	Important	No	No	2
			CVE-2022-21849	Remote Code	Important	No	No	2

				Execution				
			CVE-2022-21850	Remote Code Execution	Important	No	No	2
			CVE-2022-21922	Remote Code Execution	Important	No	No	2
			CVE-2022-21889	Denial of Service	Important	No	No	2
			CVE-2022-21905	Security Feature Bypass	Important	No	No	2
			CVE-2022-21897	Elevation of Privilege	Important	No	No	1
			CVE-2022-21958	Remote Code Execution	Important	No	No	2
			CVE-2022-21835	Elevation of Privilege	Important	No	No	2
			CVE-2022-21880	Information Disclosure	Important	No	No	2
			CVE-2022-21896	Elevation of Privilege	Important	No	No	2
			CVE-2022-21874	Remote Code Execution	Important	Yes	No	2
			CVE-2022-21902	Elevation of Privilege	Important	No	No	2
			CVE-2021-22947	Remote Code Execution	Critical	Yes	No	2
			CVE-2022-21961	Remote Code Execution	Important	No	No	2
			CVE-2022-21833	Elevation of Privilege	Critical	No	No	2
			CVE-2022-21960	Remote Code Execution	Important	No	No	2
			CVE-2022-21913	Security Feature Bypass	Important	No	No	2
			CVE-2022-21915	Information Disclosure	Important	No	No	2

		CVE-2022-21921	Security Feature Bypass	Important	No	No	2
		CVE-2022-21918	Denial of Service	Important	No	No	2
		CVE-2022-21834	Elevation of Privilege	Important	No	No	2
		CVE-2022-21887	Elevation of Privilege	Important	No	No	1
		CVE-2022-21919	Elevation of Privilege	Important	Yes	No	1
		CVE-2022-21866	Elevation of Privilege	Important	No	No	2
		CVE-2022-21881	Elevation of Privilege	Important	No	No	1
		CVE-2022-21914	Elevation of Privilege	Important	No	No	1
		CVE-2022-21906	Security Feature Bypass	Important	No	No	2
		CVE-2022-21900	Security Feature Bypass	Important	No	No	2
		CVE-2022-21883	Denial of Service	Important	No	No	2
		CVE-2022-21847	Denial of Service	Important	No	No	2
		CVE-2022-21851	Remote Code Execution	Important	No	No	2
		CVE-2022-21871	Elevation of Privilege	Important	No	No	2
		CVE-2022-21890	Denial of Service	Important	No	No	2
		CVE-2022-21862	Elevation of	Important	No	No	2

				Privilege				
			CVE-2022-21836	Spoofing	Important	Yes	No	2
			CVE-2022-21916	Elevation of Privilege	Important	No	No	1
			CVE-2022-21843	Denial of Service	Important	No	No	2
			CVE-2022-21888	Remote Code Execution	Important	No	No	2
			CVE-2022-21963	Remote Code Execution	Important	No	No	2
			CVE-2022-21882	Elevation of Privilege	Important	No	No	1
			CVE-2022-21857	Elevation of Privilege	Critical	No	No	2
			CVE-2021-36976	Remote Code Execution	Important	Yes	No	2
5009557	高危	January 11, 2022 — KB5009557 (OS Build 17763.2452) for Windows 10 Enterprise 2019 LTSC, Windows 10 IoT Enterprise 2019 LTSC, Windows 10 IoT Core 2019 LTSC	CVE-2022-21959	Remote Code Execution	Important	No	No	2
			CVE-2022-21864	Elevation of Privilege	Important	No	No	2
			CVE-2022-21898	Remote Code Execution	Critical	No	No	2
			CVE-2022-21872	Elevation of Privilege	Important	No	No	2
			CVE-2022-21870	Elevation of Privilege	Important	No	No	2
			CVE-2022-21896	Elevation of Privilege	Important	No	No	2
			CVE-2022-21874	Remote Code Execution	Important	Yes	No	2
			CVE-2021-22947	Remote Code Execution	Critical	Yes	No	2
			CVE-2022-21961	Remote Code Execution	Important	No	No	2
			CVE-2022-21833	Elevation	Critical	No	No	2

				of Privilege				
			CVE-2022-21960	Remote Code Execution	Important	No	No	2
			CVE-2022-21919	Elevation of Privilege	Important	Yes	No	1
			CVE-2022-21881	Elevation of Privilege	Important	No	No	1
			CVE-2022-21883	Denial of Service	Important	No	No	2
			CVE-2022-21875	Elevation of Privilege	Important	No	No	2
			CVE-2022-21836	Spoofing	Important	Yes	No	2
			CVE-2022-21882	Elevation of Privilege	Important	No	No	1
			CVE-2021-36976	Remote Code Execution	Important	Yes	No	2
			CVE-2022-21865	Elevation of Privilege	Important	No	No	2
			CVE-2022-21848	Denial of Service	Important	No	No	2
			CVE-2022-21861	Elevation of Privilege	Important	No	No	2
			CVE-2022-21907	Remote Code Execution	Critical	No	No	1
			CVE-2022-21962	Remote Code Execution	Important	No	No	2
			CVE-2022-21892	Remote Code Execution	Important	No	No	2
			CVE-2022-21924	Security Feature Bypass	Important	No	No	2
			CVE-2022-21877	Information Disclosure	Important	No	No	2
			CVE-2022-21908	Elevation of	Important	No	No	1

				Privilege				
			CVE-2022-21920	Elevation of Privilege	Important	No	No	2
			CVE-2022-21839	Denial of Service	Important	Yes	No	2
			CVE-2022-21850	Remote Code Execution	Important	No	No	2
			CVE-2022-21922	Remote Code Execution	Important	No	No	2
			CVE-2022-21878	Remote Code Execution	Important	No	No	2
			CVE-2022-21889	Denial of Service	Important	No	No	2
			CVE-2022-21859	Elevation of Privilege	Important	No	No	2
			CVE-2022-21868	Elevation of Privilege	Important	No	No	2
			CVE-2022-21902	Elevation of Privilege	Important	No	No	2
			CVE-2022-21918	Denial of Service	Important	No	No	2
			CVE-2022-21904	Information Disclosure	Important	No	No	2
			CVE-2022-21863	Elevation of Privilege	Important	No	No	2
			CVE-2022-21867	Elevation of Privilege	Important	No	No	2
			CVE-2022-21862	Elevation of Privilege	Important	No	No	2
			CVE-2022-21916	Elevation of Privilege	Important	No	No	1
			CVE-2022-21912	Remote Code Execution	Critical	No	No	2
			CVE-2022-21910	Elevation	Important	No	No	2

				of Privilege				
			CVE-2022-21857	Elevation of Privilege	Critical	No	No	2
			CVE-2022-21928	Remote Code Execution	Important	No	No	2
			CVE-2022-21838	Elevation of Privilege	Important	No	No	2
			CVE-2022-21852	Elevation of Privilege	Important	No	No	2
			CVE-2022-21901	Elevation of Privilege	Important	No	No	2
			CVE-2022-21903	Elevation of Privilege	Important	No	No	1
			CVE-2022-21860	Elevation of Privilege	Important	No	No	2
			CVE-2022-21897	Elevation of Privilege	Important	No	No	1
			CVE-2022-21958	Remote Code Execution	Important	No	No	2
			CVE-2022-21835	Elevation of Privilege	Important	No	No	2
			CVE-2022-21880	Information Disclosure	Important	No	No	2
			CVE-2022-21869	Elevation of Privilege	Important	No	No	2
			CVE-2022-21915	Information Disclosure	Important	No	No	2
			CVE-2022-21834	Elevation of Privilege	Important	No	No	2
			CVE-2022-21914	Elevation of	Important	No	No	1

				Privilege				
			CVE-2022-21890	Denial of Service	Important	No	No	2
			CVE-2022-21888	Remote Code Execution	Important	No	No	2
			CVE-2022-21879	Elevation of Privilege	Important	No	No	2
			CVE-2022-21894	Security Feature Bypass	Important	No	No	2
			CVE-2022-21858	Elevation of Privilege	Important	No	No	2
			CVE-2022-21873	Elevation of Privilege	Important	No	No	2
			CVE-2022-21885	Elevation of Privilege	Important	No	No	1
			CVE-2022-21925	Security Feature Bypass	Important	No	No	2
			CVE-2022-21893	Remote Code Execution	Important	No	No	2
			CVE-2022-21876	Information Disclosure	Important	No	No	2
			CVE-2022-21849	Remote Code Execution	Important	No	No	2
			CVE-2022-21905	Security Feature Bypass	Important	No	No	2
			CVE-2022-21895	Elevation of Privilege	Important	No	No	2
			CVE-2022-21913	Security Feature Bypass	Important	No	No	2
			CVE-2022-21884	Elevation of Privilege	Important	No	No	2
			CVE-2022-21866	Elevation	Important	No	No	2

				of Privilege				
			CVE-2022-21906	Security Feature Bypass	Important	No	No	2
			CVE-2022-21900	Security Feature Bypass	Important	No	No	2
			CVE-2022-21847	Denial of Service	Important	No	No	2
			CVE-2022-21851	Remote Code Execution	Important	No	No	2
			CVE-2022-21871	Elevation of Privilege	Important	No	No	2
			CVE-2022-21843	Denial of Service	Important	No	No	2
			CVE-2022-21963	Remote Code Execution	Important	No	No	2
5009601	高危	January 11, 2022 — KB5009601 (Security-only update) for Windows Server 2008 Service Pack 2	CVE-2022-21848	Denial of Service	Important	No	No	2
			CVE-2022-21885	Elevation of Privilege	Important	No	No	1
			CVE-2022-21925	Security Feature Bypass	Important	No	No	2
			CVE-2022-21924	Security Feature Bypass	Important	No	No	2
			CVE-2022-21903	Elevation of Privilege	Important	No	No	1
			CVE-2022-21908	Elevation of Privilege	Important	No	No	1
			CVE-2022-21920	Elevation of Privilege	Important	No	No	2
			CVE-2022-21850	Remote Code Execution	Important	No	No	2
			CVE-2022-21922	Remote Code	Important	No	No	2

				Execution				
			CVE-2022-21897	Elevation of Privilege	Important	No	No	1
			CVE-2022-21835	Elevation of Privilege	Important	No	No	2
			CVE-2022-21880	Information Disclosure	Important	No	No	2
			CVE-2022-21833	Elevation of Privilege	Critical	No	No	2
			CVE-2022-21915	Information Disclosure	Important	No	No	2
			CVE-2022-21913	Security Feature Bypass	Important	No	No	2
			CVE-2022-21834	Elevation of Privilege	Important	No	No	2
			CVE-2022-21919	Elevation of Privilege	Important	Yes	No	1
			CVE-2022-21884	Elevation of Privilege	Important	No	No	2
			CVE-2022-21904	Information Disclosure	Important	No	No	2
			CVE-2022-21914	Elevation of Privilege	Important	No	No	1
			CVE-2022-21851	Remote Code Execution	Important	No	No	2
			CVE-2022-21862	Elevation of Privilege	Important	No	No	2
			CVE-2022-21836	Spoofing	Important	Yes	No	2
			CVE-2022-21916	Elevation of Privilege	Important	No	No	1
			CVE-2022-21857	Elevation of	Critical	No	No	2

				Privilege				
5009546	高危	January 11, 2022 — KB5009546 (OS Build 14393.4886) for Windows 10, version 1607, all editions, Windows Server 2016, all editions	CVE-2022-21879	Elevation of Privilege	Important	No	No	2
			CVE-2022-21959	Remote Code Execution	Important	No	No	2
			CVE-2022-21928	Remote Code Execution	Important	No	No	2
			CVE-2022-21848	Denial of Service	Important	No	No	2
			CVE-2022-21894	Security Feature Bypass	Important	No	No	2
			CVE-2022-21864	Elevation of Privilege	Important	No	No	2
			CVE-2022-21873	Elevation of Privilege	Important	No	No	2
			CVE-2022-21838	Elevation of Privilege	Important	No	No	2
			CVE-2022-21885	Elevation of Privilege	Important	No	No	1
			CVE-2022-21962	Remote Code Execution	Important	No	No	2
			CVE-2022-21892	Remote Code Execution	Important	No	No	2
			CVE-2022-21925	Security Feature Bypass	Important	No	No	2
			CVE-2022-21924	Security Feature Bypass	Important	No	No	2
			CVE-2022-21901	Elevation of Privilege	Important	No	No	2
			CVE-2022-21908	Elevation of Privilege	Important	No	No	1
			CVE-2022-21903	Elevation	Important	No	No	1

				of Privilege				
			CVE-2022-21893	Remote Code Execution	Important	No	No	2
			CVE-2022-21920	Elevation of Privilege	Important	No	No	2
			CVE-2022-21876	Information Disclosure	Important	No	No	2
			CVE-2022-21870	Elevation of Privilege	Important	No	No	2
			CVE-2022-21849	Remote Code Execution	Important	No	No	2
			CVE-2022-21850	Remote Code Execution	Important	No	No	2
			CVE-2022-21922	Remote Code Execution	Important	No	No	2
			CVE-2022-21878	Remote Code Execution	Important	No	No	2
			CVE-2022-21889	Denial of Service	Important	No	No	2
			CVE-2022-21905	Security Feature Bypass	Important	No	No	2
			CVE-2022-21897	Elevation of Privilege	Important	No	No	1
			CVE-2022-21958	Remote Code Execution	Important	No	No	2
			CVE-2022-21860	Elevation of Privilege	Important	No	No	2
			CVE-2022-21859	Elevation of Privilege	Important	No	No	2
			CVE-2022-21835	Elevation of Privilege	Important	No	No	2
			CVE-2022-21880	Information Disclosure	Important	No	No	2
			CVE-2022-21868	Elevation	Important	No	No	2

				of Privilege				
			CVE-2022-21874	Remote Code Execution	Important	Yes	No	2
			CVE-2022-21964	Information Disclosure	Important	No	No	2
			CVE-2022-21895	Elevation of Privilege	Important	No	No	2
			CVE-2022-21902	Elevation of Privilege	Important	No	No	2
			CVE-2022-21961	Remote Code Execution	Important	No	No	2
			CVE-2022-21833	Elevation of Privilege	Critical	No	No	2
			CVE-2022-21960	Remote Code Execution	Important	No	No	2
			CVE-2022-21913	Security Feature Bypass	Important	No	No	2
			CVE-2022-21915	Information Disclosure	Important	No	No	2
			CVE-2022-21834	Elevation of Privilege	Important	No	No	2
			CVE-2022-21919	Elevation of Privilege	Important	Yes	No	1
			CVE-2022-21884	Elevation of Privilege	Important	No	No	2
			CVE-2022-21904	Information Disclosure	Important	No	No	2
			CVE-2022-21866	Elevation of Privilege	Important	No	No	2
			CVE-2022-21881	Elevation of Privilege	Important	No	No	1
			CVE-2022-21914	Elevation	Important	No	No	1

				of Privilege				
			CVE-2022-21863	Elevation of Privilege	Important	No	No	2
			CVE-2022-21867	Elevation of Privilege	Important	No	No	2
			CVE-2022-21883	Denial of Service	Important	No	No	2
			CVE-2022-21900	Security Feature Bypass	Important	No	No	2
			CVE-2022-21851	Remote Code Execution	Important	No	No	2
			CVE-2022-21871	Elevation of Privilege	Important	No	No	2
			CVE-2022-21890	Denial of Service	Important	No	No	2
			CVE-2022-21862	Elevation of Privilege	Important	No	No	2
			CVE-2022-21875	Elevation of Privilege	Important	No	No	2
			CVE-2022-21836	Spoofing	Important	Yes	No	2
			CVE-2022-21916	Elevation of Privilege	Important	No	No	1
			CVE-2022-21843	Denial of Service	Important	No	No	2
			CVE-2022-21910	Elevation of Privilege	Important	No	No	2
			CVE-2022-21963	Remote Code Execution	Important	No	No	2
			CVE-2022-21857	Elevation of Privilege	Critical	No	No	2
			CVE-2022-21911	Denial of Service	Important	No	No	2

5009627	高危	January 11, 2022	CVE-2022-21848	Denial of Service	Important	No	No	2
		—	CVE-2022-21885	Elevation of Privilege	Important	No	No	1
		KB5009627	CVE-2022-21925	Security Feature Bypass	Important	No	No	2
		(Monthly Rollup)	CVE-2022-21924	Security Feature Bypass	Important	No	No	2
		for Windows Server 2008 Service Pack 2	CVE-2022-21903	Elevation of Privilege	Important	No	No	1
			CVE-2022-21908	Elevation of Privilege	Important	No	No	1
			CVE-2022-21920	Elevation of Privilege	Important	No	No	2
			CVE-2022-21850	Remote Code Execution	Important	No	No	2
			CVE-2022-21922	Remote Code Execution	Important	No	No	2
			CVE-2022-21897	Elevation of Privilege	Important	No	No	1
			CVE-2022-21835	Elevation of Privilege	Important	No	No	2
			CVE-2022-21880	Information Disclosure	Important	No	No	2
			CVE-2022-21833	Elevation of Privilege	Critical	No	No	2
			CVE-2022-21915	Information Disclosure	Important	No	No	2
			CVE-2022-21913	Security Feature Bypass	Important	No	No	2
			CVE-2022-21834	Elevation of	Important	No	No	2

				Privilege				
			CVE-2022-21919	Elevation of Privilege	Important	Yes	No	1
			CVE-2022-21884	Elevation of Privilege	Important	No	No	2
			CVE-2022-21904	Information Disclosure	Important	No	No	2
			CVE-2022-21914	Elevation of Privilege	Important	No	No	1
			CVE-2022-21851	Remote Code Execution	Important	No	No	2
			CVE-2022-21862	Elevation of Privilege	Important	No	No	2
			CVE-2022-21836	Spoofing	Important	Yes	No	2
			CVE-2022-21916	Elevation of Privilege	Important	No	No	1
			CVE-2022-21857	Elevation of Privilege	Critical	No	No	2
5009595	高危	January 11, 2022 — KB5009595 (Security-only update) for Windows 8.1, Windows Server 2012 R2, Windows Embedded 8.1	CVE-2022-21959	Remote Code Execution	Important	No	No	2
			CVE-2022-21928	Remote Code Execution	Important	No	No	2
			CVE-2022-21848	Denial of Service	Important	No	No	2
			CVE-2022-21894	Security Feature Bypass	Important	No	No	2
			CVE-2022-21864	Elevation of Privilege	Important	No	No	2
			CVE-2022-21838	Elevation of Privilege	Important	No	No	2
			CVE-2022-21885	Elevation of Privilege	Important	No	No	1

		Industry Enterprise, Windows Embedded 8.1 Industry Pro	CVE-2022-21962	Remote Code Execution	Important	No	No	2
			CVE-2022-21892	Remote Code Execution	Important	No	No	2
			CVE-2022-21925	Security Feature Bypass	Important	No	No	2
			CVE-2022-21901	Elevation of Privilege	Important	No	No	2
			CVE-2022-21924	Security Feature Bypass	Important	No	No	2
			CVE-2022-21908	Elevation of Privilege	Important	No	No	1
			CVE-2022-21903	Elevation of Privilege	Important	No	No	1
			CVE-2022-21893	Remote Code Execution	Important	No	No	2
			CVE-2022-21920	Elevation of Privilege	Important	No	No	2
			CVE-2022-21870	Elevation of Privilege	Important	No	No	2
			CVE-2022-21850	Remote Code Execution	Important	No	No	2
			CVE-2022-21922	Remote Code Execution	Important	No	No	2
			CVE-2022-21905	Security Feature Bypass	Important	No	No	2
			CVE-2022-21889	Denial of Service	Important	No	No	2
			CVE-2022-21897	Elevation of Privilege	Important	No	No	1
			CVE-2022-21958	Remote Code Execution	Important	No	No	2
			CVE-2022-21859	Elevation	Important	No	No	2

				of Privilege				
			CVE-2022-21899	Security Feature Bypass	Important	No	No	2
			CVE-2022-21835	Elevation of Privilege	Important	No	No	2
			CVE-2022-21880	Information Disclosure	Important	No	No	2
			CVE-2022-21868	Elevation of Privilege	Important	No	No	2
			CVE-2022-21895	Elevation of Privilege	Important	No	No	2
			CVE-2022-21961	Remote Code Execution	Important	No	No	2
			CVE-2022-21833	Elevation of Privilege	Critical	No	No	2
			CVE-2022-21960	Remote Code Execution	Important	No	No	2
			CVE-2022-21913	Security Feature Bypass	Important	No	No	2
			CVE-2022-21915	Information Disclosure	Important	No	No	2
			CVE-2022-21834	Elevation of Privilege	Important	No	No	2
			CVE-2022-21919	Elevation of Privilege	Important	Yes	No	1
			CVE-2022-21884	Elevation of Privilege	Important	No	No	2
			CVE-2022-21904	Information Disclosure	Important	No	No	2
			CVE-2022-21881	Elevation of Privilege	Important	No	No	1

			CVE-2022-21914	Elevation of Privilege	Important	No	No	1
			CVE-2022-21867	Elevation of Privilege	Important	No	No	2
			CVE-2022-21883	Denial of Service	Important	No	No	2
			CVE-2022-21900	Security Feature Bypass	Important	No	No	2
			CVE-2022-21851	Remote Code Execution	Important	No	No	2
			CVE-2022-21890	Denial of Service	Important	No	No	2
			CVE-2022-21862	Elevation of Privilege	Important	No	No	2
			CVE-2022-21875	Elevation of Privilege	Important	No	No	2
			CVE-2022-21836	Spoofing	Important	Yes	No	2
			CVE-2022-21916	Elevation of Privilege	Important	No	No	1
			CVE-2022-21843	Denial of Service	Important	No	No	2
			CVE-2022-21963	Remote Code Execution	Important	No	No	2
			CVE-2022-21857	Elevation of Privilege	Critical	No	No	2
5009543	高危	January 11, 2022 — KB5009543 (OS Builds 19042.1466, 19043.1466, and	CVE-2022-21959	Remote Code Execution	Important	No	No	2
			CVE-2022-21864	Elevation of Privilege	Important	No	No	2
			CVE-2022-21898	Remote Code Execution	Critical	No	No	2
			CVE-2022-21872	Elevation of Privilege	Important	No	No	2

		19044.14 66) for Windows 10, version 20H2, all editions , Windows Server, version 20H2, all editions , Windows 10, version 21H1, all editions , Windows 10, version 21H2, all editions	CVE-2022-21870	Elevation of Privilege	Important	No	No	2
			CVE-2022-21896	Elevation of Privilege	Important	No	No	2
			CVE-2022-21874	Remote Code Execution	Important	Yes	No	2
			CVE-2021-22947	Remote Code Execution	Critical	Yes	No	2
			CVE-2022-21961	Remote Code Execution	Important	No	No	2
			CVE-2022-21833	Elevation of Privilege	Critical	No	No	2
			CVE-2022-21960	Remote Code Execution	Important	No	No	2
			CVE-2022-21919	Elevation of Privilege	Important	Yes	No	1
			CVE-2022-21881	Elevation of Privilege	Important	No	No	1
			CVE-2022-21883	Denial of Service	Important	No	No	2
			CVE-2022-21875	Elevation of Privilege	Important	No	No	2
			CVE-2022-21836	Spoofing	Important	Yes	No	2
			CVE-2022-21882	Elevation of Privilege	Important	No	No	1
			CVE-2021-36976	Remote Code Execution	Important	Yes	No	2
			CVE-2022-21865	Elevation of Privilege	Important	No	No	2
			CVE-2022-21848	Denial of Service	Important	No	No	2
			CVE-2022-21861	Elevation of Privilege	Important	No	No	2

		CVE-2022-21907	Remote Code Execution	Critical	No	No	1
		CVE-2022-21962	Remote Code Execution	Important	No	No	2
		CVE-2022-21892	Remote Code Execution	Important	No	No	2
		CVE-2022-21924	Security Feature Bypass	Important	No	No	2
		CVE-2022-21877	Information Disclosure	Important	No	No	2
		CVE-2022-21908	Elevation of Privilege	Important	No	No	1
		CVE-2022-21920	Elevation of Privilege	Important	No	No	2
		CVE-2022-21850	Remote Code Execution	Important	No	No	2
		CVE-2022-21922	Remote Code Execution	Important	No	No	2
		CVE-2022-21878	Remote Code Execution	Important	No	No	2
		CVE-2022-21889	Denial of Service	Important	No	No	2
		CVE-2022-21859	Elevation of Privilege	Important	No	No	2
		CVE-2022-21868	Elevation of Privilege	Important	No	No	2
		CVE-2022-21902	Elevation of Privilege	Important	No	No	2
		CVE-2022-21918	Denial of Service	Important	No	No	2
		CVE-2022-21904	Information Disclosure	Important	No	No	2
		CVE-2022-21863	Elevation of Privilege	Important	No	No	2
		CVE-2022-21867	Elevation	Important	No	No	2

				of Privilege				
			CVE-2022-21862	Elevation of Privilege	Important	No	No	2
			CVE-2022-21916	Elevation of Privilege	Important	No	No	1
			CVE-2022-21912	Remote Code Execution	Critical	No	No	2
			CVE-2022-21910	Elevation of Privilege	Important	No	No	2
			CVE-2022-21857	Elevation of Privilege	Critical	No	No	2
			CVE-2022-21928	Remote Code Execution	Important	No	No	2
			CVE-2022-21838	Elevation of Privilege	Important	No	No	2
			CVE-2022-21852	Elevation of Privilege	Important	No	No	2
			CVE-2022-21901	Elevation of Privilege	Important	No	No	2
			CVE-2022-21860	Elevation of Privilege	Important	No	No	2
			CVE-2022-21897	Elevation of Privilege	Important	No	No	1
			CVE-2022-21958	Remote Code Execution	Important	No	No	2
			CVE-2022-21835	Elevation of Privilege	Important	No	No	2
			CVE-2022-21880	Information Disclosure	Important	No	No	2
			CVE-2022-21869	Elevation of	Important	No	No	2

				Privilege				
			CVE-2022-21915	Information Disclosure	Important	No	No	2
			CVE-2022-21834	Elevation of Privilege	Important	No	No	2
			CVE-2022-21914	Elevation of Privilege	Important	No	No	1
			CVE-2022-21890	Denial of Service	Important	No	No	2
			CVE-2022-21888	Remote Code Execution	Important	No	No	2
			CVE-2022-21879	Elevation of Privilege	Important	No	No	2
			CVE-2022-21894	Security Feature Bypass	Important	No	No	2
			CVE-2022-21858	Elevation of Privilege	Important	No	No	2
			CVE-2022-21873	Elevation of Privilege	Important	No	No	2
			CVE-2022-21885	Elevation of Privilege	Important	No	No	1
			CVE-2022-21925	Security Feature Bypass	Important	No	No	2
			CVE-2022-21893	Remote Code Execution	Important	No	No	2
			CVE-2022-21876	Information Disclosure	Important	No	No	2
			CVE-2022-21849	Remote Code Execution	Important	No	No	2
			CVE-2022-21905	Security Feature Bypass	Important	No	No	2
			CVE-2022-21895	Elevation of	Important	No	No	2

				Privilege				
			CVE-2022-21913	Security Feature Bypass	Important	No	No	2
			CVE-2022-21921	Security Feature Bypass	Important	No	No	2
			CVE-2022-21884	Elevation of Privilege	Important	No	No	2
			CVE-2022-21866	Elevation of Privilege	Important	No	No	2
			CVE-2022-21906	Security Feature Bypass	Important	No	No	2
			CVE-2022-21900	Security Feature Bypass	Important	No	No	2
			CVE-2022-21847	Denial of Service	Important	No	No	2
			CVE-2022-21851	Remote Code Execution	Important	No	No	2
			CVE-2022-21871	Elevation of Privilege	Important	No	No	2
			CVE-2022-21843	Denial of Service	Important	No	No	2
			CVE-2022-21963	Remote Code Execution	Important	No	No	2
5009586	可选的高危	January 11, 2022 — KB5009586 (Monthly Rollup) for Windows Server 2012, Windows	CVE-2022-21959	Remote Code Execution	Important	No	No	2
			CVE-2022-21928	Remote Code Execution	Important	No	No	2
			CVE-2022-21848	Denial of Service	Important	No	No	2
			CVE-2022-21894	Security Feature Bypass	Important	No	No	2
			CVE-2022-21864	Elevation of Privilege	Important	No	No	2

		Embedded 8 Standard	CVE-2022-21838	Elevation of Privilege	Important	No	No	2
			CVE-2022-21885	Elevation of Privilege	Important	No	No	1
			CVE-2022-21962	Remote Code Execution	Important	No	No	2
			CVE-2022-21892	Remote Code Execution	Important	No	No	2
			CVE-2022-21925	Security Feature Bypass	Important	No	No	2
			CVE-2022-21924	Security Feature Bypass	Important	No	No	2
			CVE-2022-21903	Elevation of Privilege	Important	No	No	1
			CVE-2022-21908	Elevation of Privilege	Important	No	No	1
			CVE-2022-21893	Remote Code Execution	Important	No	No	2
			CVE-2022-21920	Elevation of Privilege	Important	No	No	2
			CVE-2022-21876	Information Disclosure	Important	No	No	2
			CVE-2022-21870	Elevation of Privilege	Important	No	No	2
			CVE-2022-21850	Remote Code Execution	Important	No	No	2
			CVE-2022-21922	Remote Code Execution	Important	No	No	2
			CVE-2022-21905	Security Feature Bypass	Important	No	No	2
			CVE-2022-21889	Denial of Service	Important	No	No	2
			CVE-2022-21897	Elevation	Important	No	No	1

				of Privilege				
			CVE-2022-21958	Remote Code Execution	Important	No	No	2
			CVE-2022-21899	Security Feature Bypass	Important	No	No	2
			CVE-2022-21835	Elevation of Privilege	Important	No	No	2
			CVE-2022-21880	Information Disclosure	Important	No	No	2
			CVE-2022-21895	Elevation of Privilege	Important	No	No	2
			CVE-2022-21961	Remote Code Execution	Important	No	No	2
			CVE-2022-21833	Elevation of Privilege	Critical	No	No	2
			CVE-2022-21960	Remote Code Execution	Important	No	No	2
			CVE-2022-21913	Security Feature Bypass	Important	No	No	2
			CVE-2022-21915	Information Disclosure	Important	No	No	2
			CVE-2022-21834	Elevation of Privilege	Important	No	No	2
			CVE-2022-21919	Elevation of Privilege	Important	Yes	No	1
			CVE-2022-21884	Elevation of Privilege	Important	No	No	2
			CVE-2022-21904	Information Disclosure	Important	No	No	2
			CVE-2022-21914	Elevation of Privilege	Important	No	No	1
			CVE-2022-21867	Elevation	Important	No	No	2

				of Privilege				
			CVE-2022-21883	Denial of Service	Important	No	No	2
			CVE-2022-21900	Security Feature Bypass	Important	No	No	2
			CVE-2022-21851	Remote Code Execution	Important	No	No	2
			CVE-2022-21890	Denial of Service	Important	No	No	2
			CVE-2022-21862	Elevation of Privilege	Important	No	No	2
			CVE-2022-21875	Elevation of Privilege	Important	No	No	2
			CVE-2022-21836	Spoofing	Important	Yes	No	2
			CVE-2022-21916	Elevation of Privilege	Important	No	No	1
			CVE-2022-21843	Denial of Service	Important	No	No	2
			CVE-2022-21963	Remote Code Execution	Important	No	No	2
			CVE-2022-21857	Elevation of Privilege	Critical	No	No	2
5009545	高危	January 11, 2022 — KB500954 5 (OS Build 18363.20 37) for Windows 10 Enterpri se, version 1909, Win	CVE-2022-21959	Remote Code Execution	Important	No	No	2
			CVE-2022-21864	Elevation of Privilege	Important	No	No	2
			CVE-2022-21898	Remote Code Execution	Critical	No	No	2
			CVE-2022-21872	Elevation of Privilege	Important	No	No	2
			CVE-2022-21870	Elevation of Privilege	Important	No	No	2
			CVE-2022-21896	Elevation	Important	No	No	2

		dows 10		of				
		Enterpri		Privilege				
		se and	CVE-2022-21874	Remote Code Execution	Important	Yes	No	2
		Educatio						
		n,	CVE-2021-22947	Remote Code Execution	Critical	Yes	No	2
		version						
		1909, Win	CVE-2022-21961	Remote Code Execution	Important	No	No	2
		dows 10						
		IoT	CVE-2022-21833	Elevation of Privilege	Critical	No	No	2
		Enterpri						
		se,	CVE-2022-21960	Remote Code Execution	Important	No	No	2
		version						
		1909	CVE-2022-21919	Elevation of Privilege	Important	Yes	No	1
			CVE-2022-21881	Elevation of Privilege	Important	No	No	1
			CVE-2022-21883	Denial of Service	Important	No	No	2
			CVE-2022-21875	Elevation of Privilege	Important	No	No	2
			CVE-2022-21836	Spoofing	Important	Yes	No	2
			CVE-2022-21882	Elevation of Privilege	Important	No	No	1
			CVE-2021-36976	Remote Code Execution	Important	Yes	No	2
			CVE-2022-21865	Elevation of Privilege	Important	No	No	2
			CVE-2022-21848	Denial of Service	Important	No	No	2
			CVE-2022-21861	Elevation of Privilege	Important	No	No	2
			CVE-2022-21962	Remote Code Execution	Important	No	No	2
			CVE-2022-21892	Remote Code Execution	Important	No	No	2

		CVE-2022-21924	Security Feature Bypass	Important	No	No	2
		CVE-2022-21877	Information Disclosure	Important	No	No	2
		CVE-2022-21908	Elevation of Privilege	Important	No	No	1
		CVE-2022-21920	Elevation of Privilege	Important	No	No	2
		CVE-2022-21850	Remote Code Execution	Important	No	No	2
		CVE-2022-21922	Remote Code Execution	Important	No	No	2
		CVE-2022-21878	Remote Code Execution	Important	No	No	2
		CVE-2022-21889	Denial of Service	Important	No	No	2
		CVE-2022-21859	Elevation of Privilege	Important	No	No	2
		CVE-2022-21868	Elevation of Privilege	Important	No	No	2
		CVE-2022-21902	Elevation of Privilege	Important	No	No	2
		CVE-2022-21918	Denial of Service	Important	No	No	2
		CVE-2022-21904	Information Disclosure	Important	No	No	2
		CVE-2022-21863	Elevation of Privilege	Important	No	No	2
		CVE-2022-21867	Elevation of Privilege	Important	No	No	2
		CVE-2022-21862	Elevation of Privilege	Important	No	No	2
		CVE-2022-21916	Elevation	Important	No	No	1

				of Privilege				
			CVE-2022-21912	Remote Code Execution	Critical	No	No	2
			CVE-2022-21857	Elevation of Privilege	Critical	No	No	2
			CVE-2022-21928	Remote Code Execution	Important	No	No	2
			CVE-2022-21838	Elevation of Privilege	Important	No	No	2
			CVE-2022-21852	Elevation of Privilege	Important	No	No	2
			CVE-2022-21901	Elevation of Privilege	Important	No	No	2
			CVE-2022-21903	Elevation of Privilege	Important	No	No	1
			CVE-2022-21860	Elevation of Privilege	Important	No	No	2
			CVE-2022-21897	Elevation of Privilege	Important	No	No	1
			CVE-2022-21958	Remote Code Execution	Important	No	No	2
			CVE-2022-21835	Elevation of Privilege	Important	No	No	2
			CVE-2022-21880	Information Disclosure	Important	No	No	2
			CVE-2022-21869	Elevation of Privilege	Important	No	No	2
			CVE-2022-21915	Information Disclosure	Important	No	No	2
			CVE-2022-21834	Elevation of Privilege	Important	No	No	2

		CVE-2022-21914	Elevation of Privilege	Important	No	No	1
		CVE-2022-21890	Denial of Service	Important	No	No	2
		CVE-2022-21888	Remote Code Execution	Important	No	No	2
		CVE-2022-21894	Security Feature Bypass	Important	No	No	2
		CVE-2022-21858	Elevation of Privilege	Important	No	No	2
		CVE-2022-21873	Elevation of Privilege	Important	No	No	2
		CVE-2022-21885	Elevation of Privilege	Important	No	No	1
		CVE-2022-21925	Security Feature Bypass	Important	No	No	2
		CVE-2022-21893	Remote Code Execution	Important	No	No	2
		CVE-2022-21876	Information Disclosure	Important	No	No	2
		CVE-2022-21849	Remote Code Execution	Important	No	No	2
		CVE-2022-21905	Security Feature Bypass	Important	No	No	2
		CVE-2022-21895	Elevation of Privilege	Important	No	No	2
		CVE-2022-21913	Security Feature Bypass	Important	No	No	2
		CVE-2022-21866	Elevation of Privilege	Important	No	No	2
		CVE-2022-21906	Security Feature	Important	No	No	2

				Bypass				
			CVE-2022-21900	Security Feature Bypass	Important	No	No	2
			CVE-2022-21847	Denial of Service	Important	No	No	2
			CVE-2022-21851	Remote Code Execution	Important	No	No	2
			CVE-2022-21871	Elevation of Privilege	Important	No	No	2
			CVE-2022-21843	Denial of Service	Important	No	No	2
			CVE-2022-21963	Remote Code Execution	Important	No	No	2
5009624	可选的高危	January 11, 2022 — KB5009624 (Monthly Rollup) for Windows 8.1, Windows Server 2012 R2, Windows Embedded 8.1 Industry Enterprise, Windows Embedded 8.1 Industry Pro	CVE-2022-21959	Remote Code Execution	Important	No	No	2
			CVE-2022-21928	Remote Code Execution	Important	No	No	2
			CVE-2022-21848	Denial of Service	Important	No	No	2
			CVE-2022-21894	Security Feature Bypass	Important	No	No	2
			CVE-2022-21864	Elevation of Privilege	Important	No	No	2
			CVE-2022-21838	Elevation of Privilege	Important	No	No	2
			CVE-2022-21885	Elevation of Privilege	Important	No	No	1
			CVE-2022-21962	Remote Code Execution	Important	No	No	2
			CVE-2022-21892	Remote Code Execution	Important	No	No	2
			CVE-2022-21925	Security Feature Bypass	Important	No	No	2
			CVE-2022-21901	Elevation of	Important	No	No	2

				Privilege				
			CVE-2022-21924	Security Feature Bypass	Important	No	No	2
			CVE-2022-21908	Elevation of Privilege	Important	No	No	1
			CVE-2022-21903	Elevation of Privilege	Important	No	No	1
			CVE-2022-21893	Remote Code Execution	Important	No	No	2
			CVE-2022-21920	Elevation of Privilege	Important	No	No	2
			CVE-2022-21870	Elevation of Privilege	Important	No	No	2
			CVE-2022-21850	Remote Code Execution	Important	No	No	2
			CVE-2022-21922	Remote Code Execution	Important	No	No	2
			CVE-2022-21905	Security Feature Bypass	Important	No	No	2
			CVE-2022-21889	Denial of Service	Important	No	No	2
			CVE-2022-21897	Elevation of Privilege	Important	No	No	1
			CVE-2022-21958	Remote Code Execution	Important	No	No	2
			CVE-2022-21859	Elevation of Privilege	Important	No	No	2
			CVE-2022-21899	Security Feature Bypass	Important	No	No	2
			CVE-2022-21835	Elevation of Privilege	Important	No	No	2
			CVE-2022-21880	Information	Important	No	No	2

				Disclosure				
			CVE-2022-21868	Elevation of Privilege	Important	No	No	2
			CVE-2022-21895	Elevation of Privilege	Important	No	No	2
			CVE-2022-21961	Remote Code Execution	Important	No	No	2
			CVE-2022-21833	Elevation of Privilege	Critical	No	No	2
			CVE-2022-21960	Remote Code Execution	Important	No	No	2
			CVE-2022-21913	Security Feature Bypass	Important	No	No	2
			CVE-2022-21915	Information Disclosure	Important	No	No	2
			CVE-2022-21834	Elevation of Privilege	Important	No	No	2
			CVE-2022-21919	Elevation of Privilege	Important	Yes	No	1
			CVE-2022-21884	Elevation of Privilege	Important	No	No	2
			CVE-2022-21904	Information Disclosure	Important	No	No	2
			CVE-2022-21881	Elevation of Privilege	Important	No	No	1
			CVE-2022-21914	Elevation of Privilege	Important	No	No	1
			CVE-2022-21867	Elevation of Privilege	Important	No	No	2
			CVE-2022-21883	Denial of Service	Important	No	No	2
			CVE-2022-21900	Security	Important	No	No	2

				Feature Bypass				
			CVE-2022-21851	Remote Code Execution	Important	No	No	2
			CVE-2022-21890	Denial of Service	Important	No	No	2
			CVE-2022-21862	Elevation of Privilege	Important	No	No	2
			CVE-2022-21875	Elevation of Privilege	Important	No	No	2
			CVE-2022-21836	Spoofing	Important	Yes	No	2
			CVE-2022-21916	Elevation of Privilege	Important	No	No	1
			CVE-2022-21843	Denial of Service	Important	No	No	2
			CVE-2022-21963	Remote Code Execution	Important	No	No	2
			CVE-2022-21857	Elevation of Privilege	Critical	No	No	2
5009585	高危	January 11, 2022 — KB5009585 (OS Build 10240.19177) for Windows 10	CVE-2022-21959	Remote Code Execution	Important	No	No	2
			CVE-2022-21928	Remote Code Execution	Important	No	No	2
			CVE-2022-21848	Denial of Service	Important	No	No	2
			CVE-2022-21894	Security Feature Bypass	Important	No	No	2
			CVE-2022-21864	Elevation of Privilege	Important	No	No	2
			CVE-2022-21873	Elevation of Privilege	Important	No	No	2
			CVE-2022-21838	Elevation of Privilege	Important	No	No	2
			CVE-2022-21885	Elevation	Important	No	No	1

				of Privilege				
			CVE-2022-21962	Remote Code Execution	Important	No	No	2
			CVE-2022-21892	Remote Code Execution	Important	No	No	2
			CVE-2022-21925	Security Feature Bypass	Important	No	No	2
			CVE-2022-21901	Elevation of Privilege	Important	No	No	2
			CVE-2022-21924	Security Feature Bypass	Important	No	No	2
			CVE-2022-21908	Elevation of Privilege	Important	No	No	1
			CVE-2022-21903	Elevation of Privilege	Important	No	No	1
			CVE-2022-21893	Remote Code Execution	Important	No	No	2
			CVE-2022-21920	Elevation of Privilege	Important	No	No	2
			CVE-2022-21876	Information Disclosure	Important	No	No	2
			CVE-2022-21870	Elevation of Privilege	Important	No	No	2
			CVE-2022-21849	Remote Code Execution	Important	No	No	2
			CVE-2022-21850	Remote Code Execution	Important	No	No	2
			CVE-2022-21922	Remote Code Execution	Important	No	No	2
			CVE-2022-21878	Remote Code Execution	Important	No	No	2
			CVE-2022-21889	Denial of Service	Important	No	No	2
			CVE-2022-21905	Security	Important	No	No	2

				Feature Bypass				
			CVE-2022-21897	Elevation of Privilege	Important	No	No	1
			CVE-2022-21958	Remote Code Execution	Important	No	No	2
			CVE-2022-21860	Elevation of Privilege	Important	No	No	2
			CVE-2022-21899	Security Feature Bypass	Important	No	No	2
			CVE-2022-21859	Elevation of Privilege	Important	No	No	2
			CVE-2022-21835	Elevation of Privilege	Important	No	No	2
			CVE-2022-21880	Information Disclosure	Important	No	No	2
			CVE-2022-21868	Elevation of Privilege	Important	No	No	2
			CVE-2022-21874	Remote Code Execution	Important	Yes	No	2
			CVE-2022-21895	Elevation of Privilege	Important	No	No	2
			CVE-2022-21961	Remote Code Execution	Important	No	No	2
			CVE-2022-21833	Elevation of Privilege	Critical	No	No	2
			CVE-2022-21960	Remote Code Execution	Important	No	No	2
			CVE-2022-21913	Security Feature Bypass	Important	No	No	2
			CVE-2022-21915	Information Disclosure	Important	No	No	2
			CVE-2022-21834	Elevation	Important	No	No	2

				of Privilege				
			CVE-2022-21919	Elevation of Privilege	Important	Yes	No	1
			CVE-2022-21904	Information Disclosure	Important	No	No	2
			CVE-2022-21866	Elevation of Privilege	Important	No	No	2
			CVE-2022-21881	Elevation of Privilege	Important	No	No	1
			CVE-2022-21914	Elevation of Privilege	Important	No	No	1
			CVE-2022-21867	Elevation of Privilege	Important	No	No	2
			CVE-2022-21883	Denial of Service	Important	No	No	2
			CVE-2022-21900	Security Feature Bypass	Important	No	No	2
			CVE-2022-21851	Remote Code Execution	Important	No	No	2
			CVE-2022-21871	Elevation of Privilege	Important	No	No	2
			CVE-2022-21890	Denial of Service	Important	No	No	2
			CVE-2022-21862	Elevation of Privilege	Important	No	No	2
			CVE-2022-21875	Elevation of Privilege	Important	No	No	2
			CVE-2022-21836	Spoofing	Important	Yes	No	2
			CVE-2022-21916	Elevation of Privilege	Important	No	No	1
			CVE-2022-21843	Denial of	Important	No	No	2

				Service				
			CVE-2022-21963	Remote Code Execution	Important	No	No	2
			CVE-2022-21857	Elevation of Privilege	Critical	No	No	2
			CVE-2022-21911	Denial of Service	Important	No	No	2
5009610	高危	January 11, 2022 — KB5009610 (Monthly Rollup) for Windows 7 Enterprise ESU, Windows 7 Professional ESU, Windows 7 Ultimate ESU, Windows Server 2008 R2 Enterprise ESU, Windows Server 2008 R2 Standard ESU, Windows Server 2008 R2 Datacenter	CVE-2022-21848	Denial of Service	Important	No	No	2
			CVE-2022-21838	Elevation of Privilege	Important	No	No	2
			CVE-2022-21885	Elevation of Privilege	Important	No	No	1
			CVE-2022-21925	Security Feature Bypass	Important	No	No	2
			CVE-2022-21924	Security Feature Bypass	Important	No	No	2
			CVE-2022-21903	Elevation of Privilege	Important	No	No	1
			CVE-2022-21908	Elevation of Privilege	Important	No	No	1
			CVE-2022-21893	Remote Code Execution	Important	No	No	2
			CVE-2022-21920	Elevation of Privilege	Important	No	No	2
			CVE-2022-21850	Remote Code Execution	Important	No	No	2
			CVE-2022-21922	Remote Code Execution	Important	No	No	2
			CVE-2022-21905	Security Feature Bypass	Important	No	No	2
			CVE-2022-21889	Denial of Service	Important	No	No	2

		er	CVE-2022-21897	Elevation of Privilege	Important	No	No	1
		ESU, Windows						
		Embedded Standard 7	CVE-2022-21859	Elevation of Privilege	Important	No	No	2
		ESU, Windows	CVE-2022-21899	Security Feature Bypass	Important	No	No	2
		Embedded POSReady 7 ESU	CVE-2022-21835	Elevation of Privilege	Important	No	No	2
			CVE-2022-21880	Information Disclosure	Important	No	No	2
			CVE-2022-21833	Elevation of Privilege	Critical	No	No	2
			CVE-2022-21915	Information Disclosure	Important	No	No	2
			CVE-2022-21913	Security Feature Bypass	Important	No	No	2
			CVE-2022-21834	Elevation of Privilege	Important	No	No	2
			CVE-2022-21919	Elevation of Privilege	Important	Yes	No	1
			CVE-2022-21884	Elevation of Privilege	Important	No	No	2
			CVE-2022-21904	Information Disclosure	Important	No	No	2
			CVE-2022-21914	Elevation of Privilege	Important	No	No	1
			CVE-2022-21900	Security Feature Bypass	Important	No	No	2
			CVE-2022-21883	Denial of Service	Important	No	No	2
			CVE-2022-21851	Remote Code	Important	No	No	2

				Execution				
			CVE-2022-21890	Denial of Service	Important	No	No	2
			CVE-2022-21862	Elevation of Privilege	Important	No	No	2
			CVE-2022-21836	Spoofing	Important	Yes	No	2
			CVE-2022-21916	Elevation of Privilege	Important	No	No	1
			CVE-2022-21843	Denial of Service	Important	No	No	2
			CVE-2022-21857	Elevation of Privilege	Critical	No	No	2
5009619	高危	January 11, 2022 — KB5009619 (Security-only update) for Windows Server 2012, Windows Embedded Standard	CVE-2022-21959	Remote Code Execution	Important	No	No	2
			CVE-2022-21928	Remote Code Execution	Important	No	No	2
			CVE-2022-21848	Denial of Service	Important	No	No	2
			CVE-2022-21894	Security Feature Bypass	Important	No	No	2
			CVE-2022-21864	Elevation of Privilege	Important	No	No	2
			CVE-2022-21838	Elevation of Privilege	Important	No	No	2
			CVE-2022-21885	Elevation of Privilege	Important	No	No	1
			CVE-2022-21962	Remote Code Execution	Important	No	No	2
			CVE-2022-21892	Remote Code Execution	Important	No	No	2
			CVE-2022-21925	Security Feature Bypass	Important	No	No	2
			CVE-2022-21924	Security Feature	Important	No	No	2

				Bypass				
			CVE-2022-21903	Elevation of Privilege	Important	No	No	1
			CVE-2022-21908	Elevation of Privilege	Important	No	No	1
			CVE-2022-21893	Remote Code Execution	Important	No	No	2
			CVE-2022-21920	Elevation of Privilege	Important	No	No	2
			CVE-2022-21876	Information Disclosure	Important	No	No	2
			CVE-2022-21870	Elevation of Privilege	Important	No	No	2
			CVE-2022-21850	Remote Code Execution	Important	No	No	2
			CVE-2022-21922	Remote Code Execution	Important	No	No	2
			CVE-2022-21905	Security Feature Bypass	Important	No	No	2
			CVE-2022-21889	Denial of Service	Important	No	No	2
			CVE-2022-21897	Elevation of Privilege	Important	No	No	1
			CVE-2022-21958	Remote Code Execution	Important	No	No	2
			CVE-2022-21899	Security Feature Bypass	Important	No	No	2
			CVE-2022-21835	Elevation of Privilege	Important	No	No	2
			CVE-2022-21880	Information Disclosure	Important	No	No	2
			CVE-2022-21895	Elevation of Privilege	Important	No	No	2

		CVE-2022-21961	Remote Code Execution	Important	No	No	2
		CVE-2022-21833	Elevation of Privilege	Critical	No	No	2
		CVE-2022-21960	Remote Code Execution	Important	No	No	2
		CVE-2022-21913	Security Feature Bypass	Important	No	No	2
		CVE-2022-21915	Information Disclosure	Important	No	No	2
		CVE-2022-21834	Elevation of Privilege	Important	No	No	2
		CVE-2022-21919	Elevation of Privilege	Important	Yes	No	1
		CVE-2022-21884	Elevation of Privilege	Important	No	No	2
		CVE-2022-21904	Information Disclosure	Important	No	No	2
		CVE-2022-21914	Elevation of Privilege	Important	No	No	1
		CVE-2022-21867	Elevation of Privilege	Important	No	No	2
		CVE-2022-21883	Denial of Service	Important	No	No	2
		CVE-2022-21900	Security Feature Bypass	Important	No	No	2
		CVE-2022-21851	Remote Code Execution	Important	No	No	2
		CVE-2022-21890	Denial of Service	Important	No	No	2
		CVE-2022-21862	Elevation of Privilege	Important	No	No	2
		CVE-2022-21875	Elevation	Important	No	No	2

				of Privilege				
			CVE-2022-21836	Spoofing	Important	Yes	No	2
			CVE-2022-21916	Elevation of Privilege	Important	No	No	1
			CVE-2022-21843	Denial of Service	Important	No	No	2
			CVE-2022-21963	Remote Code Execution	Important	No	No	2
			CVE-2022-21857	Elevation of Privilege	Critical	No	No	2

本月微软发布的软件安全更新补丁共 40 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
5002128	高危	Excel 2013	CVE-2022-21840	Remote Code Execution	Critical	No	No	2
5002114	高危	Excel 2016	CVE-2022-21840	Remote Code Execution	Critical	No	No	2
5008631	高危	Exchange Server 2019, 2016, and 2013	CVE-2022-21846	Remote Code Execution	Critical	No	No	1
			CVE-2022-21969	Remote Code Execution	Important	No	No	1
			CVE-2022-21855	Remote Code Execution	Important	No	No	1
4462205	高危	Office 2013	CVE-2022-21840	Remote Code Execution	Critical	No	No	2
5002064	高危	Office 2013	CVE-2022-21840	Remote	Critical	No	No	2

				Code Execution				
5002119	高危	Office 2013	CVE-2022-21841	Remote Code Execution	Important	No	No	2
5002124	高危	Office 2013	CVE-2022-21840	Remote Code Execution	Critical	No	No	2
5002052	高危	Office 2016	CVE-2022-21840	Remote Code Execution	Critical	No	No	2
5002060	高危	Office 2016	CVE-2022-21840	Remote Code Execution	Critical	No	No	2
5002115	高危	Office 2016	CVE-2022-21840	Remote Code Execution	Critical	No	No	2
5002116	高危	Office 2016	CVE-2022-21841	Remote Code Execution	Important	No	No	2
5002122	高危	Office Web Apps Server 2013	CVE-2022-21840	Remote Code Execution	Critical	No	No	2
5001995	高危	SharePoint Enterprise Server 2013	CVE-2022-21840	Remote Code Execution	Critical	No	No	2
5002102	高危	SharePoint Enterprise Server 2013	CVE-2022-21840	Remote Code Execution	Critical	No	No	2
5002113	高危	SharePoint Enterprise Server 2016	CVE-2022-21837	Remote Code Execution	Important	No	No	2
			CVE-2022-21840	Remote Code Execution	Critical	No	No	2
			CVE-2022-21842	Remote Code Execution	Important	No	No	2
5002118	高危	SharePoint Enterprise Server 2016	CVE-2022-21840	Remote Code Execution	Critical	No	No	2
			CVE-2022-21842	Remote	Important	No	No	2

				Code Execution				
5002127	高危	SharePoint Foundation 2013	CVE-2022-21837	Remote Code Execution	Important	No	No	2
			CVE-2022-21840	Remote Code Execution	Critical	No	No	2
5002129	高危	SharePoint Foundation 2013	CVE-2022-21840	Remote Code Execution	Critical	No	No	2
5002057	高危	Word 2016	CVE-2022-21842	Remote Code Execution	Important	No	No	2
5008876	高危	January 11, 2022-KB5008876 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-2022-21911	Denial of Service	Important	No	No	2
5008877	高危	January 11, 2022-KB5008877 Cumulative Update for .NET Framework	CVE-2022-21911	Denial of Service	Important	No	No	2

		4.8 for Windows 10, version 1607 and Windows Server, version 2016						
5008879	高危	January 11, 2022-KB5008879 Cumulative Update for .NET Framework 3.5 and 4.8 for Windows 10, version 1909	CVE-2022-21911	Denial of Service	Important	No	No	2
5008880	高危	January 11, 2022-KB5008880 Cumulative Update for .NET Framework 3.5 and 4.8 for Windows 11	CVE-2022-21911	Denial of Service	Important	No	No	2
5009718	高危	January 11, 2022-KB5009718 Cumulative Update for .NET Framework 3.5, 4.7.2 and 4.8 for Windows 10, version 1809 and Windows	CVE-2022-21911	Denial of Service	Important	No	No	2

		Server, version 2019						
5009722	高危	Security and Quality Rollup for .NET Framework 2.0, 3.0, 4.5.2, 4.6 and 4.6.2 for Windows Server 2008 SP2 (KB5009722)	CVE-2022-21911	Denial of Service	Important	No	No	2
5009721	高危	Security and Quality Rollup for .NET Framework 3.5, 4.5.2, 4.6, 4.6.1, 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 (KB5009721)	CVE-2022-21911	Denial of Service	Important	No	No	2
5009720	高危	Security and Quality Rollup for .NET Framework 3.5, 4.5.2, 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Windows	CVE-2022-21911	Denial of Service	Important	No	No	2

		Server 2012 (KB5009720)						
5009719	高危	Security and Quality Rollup for .NET Framework 3.5.1, 4.5.2, 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Windows 7 SP1 and Windows Server 2008 R2 SP1 (KB5009719)	CVE-2022-21911	Denial of Service	Important	No	No	2
5009714	高危	Security Only Update for .NET Framework 2.0, 3.0, 4.5.2, 4.6 and 4.6.2 for Windows Server 2008 SP2 (KB5009714)	CVE-2022-21911	Denial of Service	Important	No	No	2
5008891	高危	Security Only Update for .NET Framework 3.5 for Windows 8.1 and Windows Server 2012 R2 (KB5008891)	CVE-2022-21911	Denial of Service	Important	No	No	2
5008888	高危	Security Only Update	CVE-2022-21911	Denial of Service	Important	No	No	2

		for .NET Framework 3.5 for Windows Server 2012 (KB5008888)						
5009713	高危	Security Only Update for .NET Framework 3.5, 4.5.2, 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Windows 8.1 and Windows Server 2012 R2 (KB5009713)	CVE-2022-21911	Denial of Service	Important	No	No	2
5009712	高危	Security Only Update for .NET Framework 3.5, 4.5.2, 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Windows Server 2012 (KB5009712)	CVE-2022-21911	Denial of Service	Important	No	No	2
5009711	高危	Security Only Update for .NET Framework 3.5.1, 4.5.2, 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1,	CVE-2022-21911	Denial of Service	Important	No	No	2

		4.7.2, 4.8 for Windows 7 SP1 and Windows Server 2008 R2 SP1 (KB5009711)						
5008893	高危	Security Only Update for .NET Framework 4.5.2 for Windows 8.1 and Windows Server 2012 R2 (KB5008893)	CVE-2022-21911	Denial of Service	Important	No	No	2
5008892	高危	Security Only Update for .NET Framework 4.5.2 for Windows Server 2012 (KB5008892)	CVE-2022-21911	Denial of Service	Important	No	No	2
5008895	高危	Security Only Update for .NET Framework 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2 for Windows 8.1 and Windows Server 2012 R2 (KB5008895)	CVE-2022-21911	Denial of Service	Important	No	No	2
5008894	高危	Security Only Update for .NET Framework	CVE-2022-21911	Denial of Service	Important	No	No	2

		4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2 for Windows Server 2012 (KB5008894)						
5008897	高危	Security Only Update for .NET Framework 4.8 for Windows 8.1 and Windows Server 2012 R2 (KB5008897)	CVE-2022-21911	Denial of Service	Important	No	No	2
5008896	高危	Security Only Update for .NET Framework 4.8 for Windows Server 2012 (KB5008896)	CVE-2022-21911	Denial of Service	Important	No	No	2

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
4504713	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>