奇安信集团 2022 年 10 月补丁库

更新通告

第一次更新

奇安信集团漏洞补丁运营团队

2022 年 10 月 12 日

目 录

文档信息

文档名称	奇安信集团 2022 年 10 月补丁库更新通告		
文档编号	Qi An Xin Group-MSPatch-2022-1012		
发布日期	2022-10-12	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:2022.10.12.1,V10版本:2022.10.12.1001)已发布，本次更新推送了19个微软安全补丁，修复了71个安全漏洞，其中11个微软官方评级为“严重(Critical)”，60个评级为“重要(Important)”，这些漏洞影响产品Windows和Microsoft Office。同时推送了2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 22 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
5018410	CVE-2022-37987	Elevation of Privilege	Important	No	No	Exploitation More Likely
5018478						
5018419						
5018427						
5018457						
5018454						
5018425						
5018446						
5018479						
5018450						
5018411						
5018418						
5018474						
5018476						
5018410	CVE-2022-30198	Remote Code Execution	Critical	No	No	Exploitation Less Likely
5018478						
5018419						
5018427						
5018457						
5018454						
5018425						
5018479						
5018411						
5018418						
5018474						
5018476						
5018410	CVE-2022-38047					

5018478 5018419 5018427 5018457 5018454 5018425 5018446 5018479 5018450 5018411 5018418 5018474 5018476		Remote Code Execution	Critical	No	No	Exploitation Less Likely
5018410 5018419 5018427 5018418	CVE-2022-37970	Elevation of Privilege	Important	No	No	Exploitation More Likely
5018410 5018419 5018418	CVE-2022-38050	Elevation of Privilege	Important	No	No	Exploitation More Likely
5018410 5018478 5018419 5018427 5018457 5018454 5018425 5018446 5018479 5018450 5018411 5018418 5018474 5018476	CVE-2022-41033	Elevation of Privilege	Important	No	Yes	Exploitation Detected
5018410 5018478 5018419 5018427 5018457	CVE-2022-38000	Remote Code Execution	Critical	No	No	Exploitation Less Likely

5018454 5018425 5018479 5018411 5018418 5018474 5018476						
5018410 5018478 5018419 5018427 5018457 5018454 5018425 5018446 5018479 5018450 5018411 5018418 5018474 5018476	CVE-2022-41081	Remote Code Execution	Critical	No	No	Exploitation Less Likely
5018410 5018478 5018419 5018427 5018457 5018425 5018411 5018418 5018474 5018476	CVE-2022-38028	Elevation of Privilege	Important	No	No	Exploitation More Likely
5018410 5018478 5018419 5018427 5018457 5018454 5018425 5018446 5018479 5018450	CVE-2022-37997	Elevation of Privilege	Important	No	No	Exploitation More Likely

5018411 5018418 5018474 5018476						
5018410 5018478 5018419 5018427 5018457 5018454 5018425 5018446 5018479 5018450 5018411 5018418 5018474 5018476	CVE-2022-24504	Remote Code Execution	Critical	No	No	Exploitation Less Likely
5018410 5018427 5018418	CVE-2022-37974	Information Disclosure	Important	No	No	Exploitation More Likely
5018410 5018478 5018419 5018457 5018454 5018425 5018446 5018479 5018450 5018411 5018418 5018474 5018476	CVE-2022-38051	Elevation of Privilege	Important	No	No	Exploitation More Likely
5018410 5018419 5018427 5018411 5018418	CVE-2022-37979	Elevation of Privilege	Critical	No	No	Exploitation Less Likely

5018410 5018478 5018419 5018427 5018457 5018454 5018425 5018479 5018411 5018418 5018474 5018476	CVE-2022-22035	Remote Code Execution	Critical	No	No	Exploitation Less Likely
5018410 5018478 5018419 5018427 5018457 5018454 5018425 5018446 5018479 5018450 5018411 5018418 5018474 5018476	CVE-2022-37989	Elevation of Privilege	Important	No	No	Exploitation More Likely
5018410 5018478 5018419 5018427 5018457 5018454 5018425 5018446 5018479 5018450 5018411 5018418 5018474 5018476	CVE-2022-33634	Remote Code Execution	Critical	No	No	Exploitation Less Likely
5018478	CVE-2022-37976					

5018419 5018457 5018454 5018446 5018479 5018450 5018411 5018474 5018476		Elevation of Privilege	Critical	No	No	Exploitation Less Likely
5002279 5002026 5002288	CVE-2022-38048	Remote Code Execution	Critical	No	No	Exploitation Less Likely
5002287 5002284	CVE-2022-38053	Remote Code Execution	Important	No	No	Exploitation More Likely
5002287 5002284	CVE-2022-41036	Remote Code Execution	Important	No	No	Exploitation More Likely
5002287 5002284	CVE-2022-41038	Remote Code Execution	Critical	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
5018410	高危	October 11, 2022—KB5018410 (OS Builds 19042.2130, 19043.2130, and 19044.2130) for Windows 10 Enterprise Multi-Session, version 20H2, Windows 10 Enterprise and Education, version 20H2, Windows 10 IoT Enterpri	CVE-2022-37982	Remote Code Execution	Important	No	No	2
			CVE-2022-38027	Elevation of Privilege	Important	No	No	2
			CVE-2022-38033	Information Disclosure	Important	No	No	2
			CVE-2022-37975	Elevation of Privilege	Important	No	No	2
			CVE-2022-38034	Elevation of Privilege	Important	No	No	2
			CVE-2022-37999	Elevation of Privilege	Important	No	No	2
			CVE-2022-37988	Elevation of Privilege	Important	No	No	2
			CVE-2022-38022	Elevation of Privilege	Important	No	No	2
			CVE-2022-37984	Elevation of Privilege	Important	No	No	2
			CVE-2022-35770	Spoofing	Important	No	No	2
			CVE-2022-37981	Denial of Service	Important	No	No	2
			CVE-2022-37996	Information Disclosure	Important	No	No	2

		se, version 20H2,Windows 10 on Surface Hub,Windows 10, version 21H1, all editions,Windows 10, version 21H2, all editions	CVE-2022-37987	Elevation of Privilege	Important	No	No	1
			CVE-2022-37991	Elevation of Privilege	Important	No	No	2
			CVE-2022-30198	Remote Code Execution	Critical	No	No	2
			CVE-2022-38038	Elevation of Privilege	Important	No	No	2
			CVE-2022-38042	Elevation of Privilege	Important	No	No	2
			CVE-2022-33635	Remote Code Execution	Important	No	No	2
			CVE-2022-38047	Remote Code Execution	Critical	No	No	2
			CVE-2022-37993	Elevation of Privilege	Important	No	No	2
			CVE-2022-38046	Information Disclosure	Important	No	No	2
			CVE-2022-37970	Elevation of Privilege	Important	No	No	1
			CVE-2022-38016	Elevation of Privilege	Important	No	No	2
			CVE-2022-37978	Security Feature Bypass	Important	No	No	2
			CVE-2022-38039	Elevation of Privilege	Important	No	No	2
			CVE-2022-38003	Elevation of Privilege	Important	No	No	2
			CVE-2022-38050	Elevation of Privilege	Important	No	No	1

			CVE-2022-37994	Elevation of Privilege	Important	No	No	2
			CVE-2022-37983	Elevation of Privilege	Important	No	No	2
			CVE-2022-37998	Denial of Service	Important	No	No	2
			CVE-2022-37965	Denial of Service	Important	No	No	2
			CVE-2022-41033	Elevation of Privilege	Important	No	Yes	0
			CVE-2022-38000	Remote Code Execution	Critical	No	No	2
			CVE-2022-37973	Denial of Service	Important	No	No	2
			CVE-2022-41081	Remote Code Execution	Critical	No	No	2
			CVE-2022-38040	Remote Code Execution	Important	No	No	2
			CVE-2022-38045	Elevation of Privilege	Important	No	No	2
			CVE-2022-38028	Elevation of Privilege	Important	No	No	1
			CVE-2022-38037	Elevation of Privilege	Important	No	No	2
			CVE-2022-37990	Elevation of Privilege	Important	No	No	2
			CVE-2022-38029	Elevation of Privilege	Important	No	No	2
			CVE-2022-37980	Elevation of Privilege	Important	No	No	2
			CVE-2022-38021	Elevation of Privilege	Important	No	No	2

			CVE-2022-38043	Information Disclosure	Important	No	No	2
			CVE-2022-37997	Elevation of Privilege	Important	No	No	1
			CVE-2022-37985	Information Disclosure	Important	No	No	2
			CVE-2022-24504	Remote Code Execution	Critical	No	No	2
			CVE-2022-37977	Denial of Service	Important	No	No	2
			CVE-2022-37974	Information Disclosure	Important	No	No	1
			CVE-2022-38051	Elevation of Privilege	Important	No	No	1
			CVE-2022-38044			No	No	2
			CVE-2022-38026	Information Disclosure	Important	No	No	2
			CVE-2022-37979	Elevation of Privilege	Critical	No	No	2
			CVE-2022-22035	Remote Code Execution	Critical	No	No	2
			CVE-2022-33645	Denial of Service	Important	No	No	2
			CVE-2022-37989	Elevation of Privilege	Important	No	No	1
			CVE-2022-38041	Denial of Service	Important	No	No	2
			CVE-2022-38030	Information Disclosure	Important	No	No	2
			CVE-2022-38031	Remote Code Execution	Important	No	No	2
			CVE-2022-37995	Elevation of Privilege	Important	No	No	2
			CVE-2022-38032	Security Feature Bypass	Important	No	No	2

			CVE-2022-33634	Remote Code Execution	Critical	No	No	2
			CVE-2022-37986	Elevation of Privilege	Important	No	No	2
5018478	高危	October 11, 2022—KB5018478 (Security-only update) for Windows Server 2012,Windows Embedded 8 Standard	CVE-2022-37982	Remote Code Execution	Important	No	No	2
			CVE-2022-38027	Elevation of Privilege	Important	No	No	2
			CVE-2022-38033	Information Disclosure	Important	No	No	2
			CVE-2022-37975	Elevation of Privilege	Important	No	No	2
			CVE-2022-38034	Elevation of Privilege	Important	No	No	2
			CVE-2022-37999	Elevation of Privilege	Important	No	No	2
			CVE-2022-37988	Elevation of Privilege	Important	No	No	2
			CVE-2022-38022	Elevation of Privilege	Important	No	No	2
			CVE-2022-37984	Elevation of Privilege	Important	No	No	2
			CVE-2022-35770	Spoofing	Important	No	No	2
			CVE-2022-37981	Denial of Service	Important	No	No	2
			CVE-2022-37987	Elevation of Privilege	Important	No	No	1
			CVE-2022-37991	Elevation of Privilege	Important	No	No	2
			CVE-2022-30198	Remote Code Execution	Critical	No	No	2

			CVE-2022-38038	Elevation of Privilege	Important	No	No	2
			CVE-2022-38042	Elevation of Privilege	Important	No	No	2
			CVE-2022-33635	Remote Code Execution	Important	No	No	2
			CVE-2022-38047	Remote Code Execution	Critical	No	No	2
			CVE-2022-37993	Elevation of Privilege	Important	No	No	2
			CVE-2022-37978	Security Feature Bypass	Important	No	No	2
			CVE-2022-38000	Remote Code Execution	Critical	No	No	2
			CVE-2022-37994	Elevation of Privilege	Important	No	No	2
			CVE-2022-37965	Denial of Service	Important	No	No	2
			CVE-2022-41033	Elevation of Privilege	Important	No	Yes	0
			CVE-2022-41081	Remote Code Execution	Critical	No	No	2
			CVE-2022-38040	Remote Code Execution	Important	No	No	2
			CVE-2022-38045	Elevation of Privilege	Important	No	No	2
			CVE-2022-38028	Elevation of Privilege	Important	No	No	1
			CVE-2022-37976	Elevation of Privilege	Critical	No	No	2
			CVE-2022-38037	Elevation of Privilege	Important	No	No	2

			CVE-2022-37990	Elevation of Privilege	Important	No	No	2
			CVE-2022-38029	Elevation of Privilege	Important	No	No	2
			CVE-2022-37985	Information Disclosure	Important	No	No	2
			CVE-2022-37997	Elevation of Privilege	Important	No	No	1
			CVE-2022-38043	Information Disclosure	Important	No	No	2
			CVE-2022-24504	Remote Code Execution	Critical	No	No	2
			CVE-2022-37977	Denial of Service	Important	No	No	2
			CVE-2022-38051	Elevation of Privilege	Important	No	No	1
			CVE-2022-38044			No	No	2
			CVE-2022-38026	Information Disclosure	Important	No	No	2
			CVE-2022-22035	Remote Code Execution	Critical	No	No	2
			CVE-2022-33645	Denial of Service	Important	No	No	2
			CVE-2022-37989	Elevation of Privilege	Important	No	No	1
			CVE-2022-38041	Denial of Service	Important	No	No	2
			CVE-2022-38031	Remote Code Execution	Important	No	No	2
			CVE-2022-38032	Security Feature Bypass	Important	No	No	2
			CVE-2022-33634	Remote Code Execution	Critical	No	No	2
			CVE-2022-37986	Elevation of Privilege	Important	No	No	2

5018419	高危	October 11, 2022—KB5018419 (OS Build 17763.3532) for Windows 10 Enterprise 2019 LTSC,Windows 10 IoT Enterprise 2019 LTSC,Windows 10 IoT Core 2019 LTSC,Windows Server 2019	CVE-2022-37982	Remote Code Execution	Important	No	No	2
			CVE-2022-38027	Elevation of Privilege	Important	No	No	2
			CVE-2022-38033	Information Disclosure	Important	No	No	2
			CVE-2022-37975	Elevation of Privilege	Important	No	No	2
			CVE-2022-38034	Elevation of Privilege	Important	No	No	2
			CVE-2022-37999	Elevation of Privilege	Important	No	No	2
			CVE-2022-37988	Elevation of Privilege	Important	No	No	2
			CVE-2022-38022	Elevation of Privilege	Important	No	No	2
			CVE-2022-37984	Elevation of Privilege	Important	No	No	2
			CVE-2022-35770	Spoofing	Important	No	No	2
			CVE-2022-37981	Denial of Service	Important	No	No	2
			CVE-2022-37996	Information Disclosure	Important	No	No	2
			CVE-2022-37987	Elevation of Privilege	Important	No	No	1
			CVE-2022-37991	Elevation of Privilege	Important	No	No	2
			CVE-2022-30198	Remote Code Execution	Critical	No	No	2
			CVE-2022-38038	Elevation of Privilege	Important	No	No	2

			CVE-2022-38042	Elevation of Privilege	Important	No	No	2
			CVE-2022-33635	Remote Code Execution	Important	No	No	2
			CVE-2022-38047	Remote Code Execution	Critical	No	No	2
			CVE-2022-37993	Elevation of Privilege	Important	No	No	2
			CVE-2022-38046	Information Disclosure	Important	No	No	2
			CVE-2022-37970	Elevation of Privilege	Important	No	No	1
			CVE-2022-38016	Elevation of Privilege	Important	No	No	2
			CVE-2022-37978	Security Feature Bypass	Important	No	No	2
			CVE-2022-38039	Elevation of Privilege	Important	No	No	2
			CVE-2022-38003	Elevation of Privilege	Important	No	No	2
			CVE-2022-38050	Elevation of Privilege	Important	No	No	1
			CVE-2022-37994	Elevation of Privilege	Important	No	No	2
			CVE-2022-37983	Elevation of Privilege	Important	No	No	2
			CVE-2022-38000	Remote Code Execution	Critical	No	No	2
			CVE-2022-37965	Denial of Service	Important	No	No	2

			CVE-2022-41033	Elevation of Privilege	Important	No	Yes	0
			CVE-2022-41081	Remote Code Execution	Critical	No	No	2
			CVE-2022-38040	Remote Code Execution	Important	No	No	2
			CVE-2022-38045	Elevation of Privilege	Important	No	No	2
			CVE-2022-37976	Elevation of Privilege	Critical	No	No	2
			CVE-2022-38028	Elevation of Privilege	Important	No	No	1
			CVE-2022-38037	Elevation of Privilege	Important	No	No	2
			CVE-2022-37990	Elevation of Privilege	Important	No	No	2
			CVE-2022-38029	Elevation of Privilege	Important	No	No	2
			CVE-2022-38021	Elevation of Privilege	Important	No	No	2
			CVE-2022-38043	Information Disclosure	Important	No	No	2
			CVE-2022-37985	Information Disclosure	Important	No	No	2
			CVE-2022-37997	Elevation of Privilege	Important	No	No	1
			CVE-2022-24504	Remote Code Execution	Critical	No	No	2
			CVE-2022-37977	Denial of Service	Important	No	No	2
			CVE-2022-38051	Elevation of Privilege	Important	No	No	1

			CVE-2022-38044			No	No	2
			CVE-2022-38026	Information Disclosure	Important	No	No	2
			CVE-2022-37979	Elevation of Privilege	Critical	No	No	2
			CVE-2022-22035	Remote Code Execution	Critical	No	No	2
			CVE-2022-33645	Denial of Service	Important	No	No	2
			CVE-2022-37989	Elevation of Privilege	Important	No	No	1
			CVE-2022-38041	Denial of Service	Important	No	No	2
			CVE-2022-38030	Information Disclosure	Important	No	No	2
			CVE-2022-38031	Remote Code Execution	Important	No	No	2
			CVE-2022-37995	Elevation of Privilege	Important	No	No	2
			CVE-2022-38032	Security Feature Bypass	Important	No	No	2
			CVE-2022-33634	Remote Code Execution	Critical	No	No	2
			CVE-2022-37986	Elevation of Privilege	Important	No	No	2
5018427	高危	October 11, 2022—KB5018427 (OS Build 22621.674) for Windows 11	CVE-2022-37982	Remote Code Execution	Important	No	No	2
			CVE-2022-38027	Elevation of Privilege	Important	No	No	2
			CVE-2022-38033	Information Disclosure	Important	No	No	2
			CVE-2022-37975	Elevation of Privilege	Important	No	No	2

		version 22H2, all editions	CVE-2022-38034	Elevation of Privilege	Important	No	No	2
			CVE-2022-37999	Elevation of Privilege	Important	No	No	2
			CVE-2022-37988	Elevation of Privilege	Important	No	No	2
			CVE-2022-38022	Elevation of Privilege	Important	No	No	2
			CVE-2022-37984	Elevation of Privilege	Important	No	No	2
			CVE-2022-35770	Spoofing	Important	No	No	2
			CVE-2022-38025	Information Disclosure	Important	No	No	2
			CVE-2022-37981	Denial of Service	Important	No	No	2
			CVE-2022-37996	Information Disclosure	Important	No	No	2
			CVE-2022-37987	Elevation of Privilege	Important	No	No	1
			CVE-2022-37991	Elevation of Privilege	Important	No	No	2
			CVE-2022-30198	Remote Code Execution	Critical	No	No	2
			CVE-2022-38038	Elevation of Privilege	Important	No	No	2
			CVE-2022-38042	Elevation of Privilege	Important	No	No	2
			CVE-2022-38047	Remote Code Execution	Critical	No	No	2
			CVE-2022-37993	Elevation of Privilege	Important	No	No	2

			CVE-2022-37970	Elevation of Privilege	Important	No	No	1
			CVE-2022-38016	Elevation of Privilege	Important	No	No	2
			CVE-2022-37978	Security Feature Bypass	Important	No	No	2
			CVE-2022-38039	Elevation of Privilege	Important	No	No	2
			CVE-2022-38000	Remote Code Execution	Critical	No	No	2
			CVE-2022-37994	Elevation of Privilege	Important	No	No	2
			CVE-2022-37983	Elevation of Privilege	Important	No	No	2
			CVE-2022-37998	Denial of Service	Important	No	No	2
			CVE-2022-37965	Denial of Service	Important	No	No	2
			CVE-2022-41033	Elevation of Privilege	Important	No	Yes	0
			CVE-2022-37973	Denial of Service	Important	No	No	2
			CVE-2022-41081	Remote Code Execution	Critical	No	No	2
			CVE-2022-38040	Remote Code Execution	Important	No	No	2
			CVE-2022-38045	Elevation of Privilege	Important	No	No	2
			CVE-2022-38028	Elevation of Privilege	Important	No	No	1
			CVE-2022-38037	Elevation of Privilege	Important	No	No	2

			CVE-2022-37990	Elevation of Privilege	Important	No	No	2
			CVE-2022-38029	Elevation of Privilege	Important	No	No	2
			CVE-2022-37980	Elevation of Privilege	Important	No	No	2
			CVE-2022-38021	Elevation of Privilege	Important	No	No	2
			CVE-2022-37985	Information Disclosure	Important	No	No	2
			CVE-2022-38043	Information Disclosure	Important	No	No	2
			CVE-2022-37997	Elevation of Privilege	Important	No	No	1
			CVE-2022-24504	Remote Code Execution	Critical	No	No	2
			CVE-2022-37977	Denial of Service	Important	No	No	2
			CVE-2022-37974	Information Disclosure	Important	No	No	1
			CVE-2022-38044			No	No	2
			CVE-2022-38026	Information Disclosure	Important	No	No	2
			CVE-2022-37979	Elevation of Privilege	Critical	No	No	2
			CVE-2022-22035	Remote Code Execution	Critical	No	No	2
			CVE-2022-33645	Denial of Service	Important	No	No	2
			CVE-2022-37989	Elevation of Privilege	Important	No	No	1
			CVE-2022-38041	Denial of Service	Important	No	No	2
			CVE-2022-33634	Remote Code Execution	Critical	No	No	2

			CVE-2022-38031	Remote Code Execution	Important	No	No	2
			CVE-2022-37995	Elevation of Privilege	Important	No	No	2
			CVE-2022-38030	Information Disclosure	Important	No	No	2
			CVE-2022-38032	Security Feature Bypass	Important	No	No	2
			CVE-2022-33635	Remote Code Execution	Important	No	No	2
			CVE-2022-37986	Elevation of Privilege	Important	No	No	2
5018457	高危	October 11, 2022—KB5018457 (Monthly Rollup) for Windows Server 2012,Windows Embedded 8 Standard	CVE-2022-37982	Remote Code Execution	Important	No	No	2
			CVE-2022-38027	Elevation of Privilege	Important	No	No	2
			CVE-2022-38033	Information Disclosure	Important	No	No	2
			CVE-2022-37975	Elevation of Privilege	Important	No	No	2
			CVE-2022-38034	Elevation of Privilege	Important	No	No	2
			CVE-2022-37999	Elevation of Privilege	Important	No	No	2
			CVE-2022-37988	Elevation of Privilege	Important	No	No	2
			CVE-2022-38022	Elevation of Privilege	Important	No	No	2
			CVE-2022-37984	Elevation of Privilege	Important	No	No	2
			CVE-2022-35770	Spoofing	Important	No	No	2

			CVE-2022-37981	Denial of Service	Important	No	No	2
			CVE-2022-37987	Elevation of Privilege	Important	No	No	1
			CVE-2022-37991	Elevation of Privilege	Important	No	No	2
			CVE-2022-30198	Remote Code Execution	Critical	No	No	2
			CVE-2022-38038	Elevation of Privilege	Important	No	No	2
			CVE-2022-38042	Elevation of Privilege	Important	No	No	2
			CVE-2022-33635	Remote Code Execution	Important	No	No	2
			CVE-2022-38047	Remote Code Execution	Critical	No	No	2
			CVE-2022-37993	Elevation of Privilege	Important	No	No	2
			CVE-2022-37978	Security Feature Bypass	Important	No	No	2
			CVE-2022-38000	Remote Code Execution	Critical	No	No	2
			CVE-2022-37994	Elevation of Privilege	Important	No	No	2
			CVE-2022-37965	Denial of Service	Important	No	No	2
			CVE-2022-41033	Elevation of Privilege	Important	No	Yes	0
			CVE-2022-41081	Remote Code Execution	Critical	No	No	2
			CVE-2022-38040	Remote Code Execution	Important	No	No	2

			CVE-2022-38045	Elevation of Privilege	Important	No	No	2
			CVE-2022-38028	Elevation of Privilege	Important	No	No	1
			CVE-2022-37976	Elevation of Privilege	Critical	No	No	2
			CVE-2022-38037	Elevation of Privilege	Important	No	No	2
			CVE-2022-37990	Elevation of Privilege	Important	No	No	2
			CVE-2022-38029	Elevation of Privilege	Important	No	No	2
			CVE-2022-37985	Information Disclosure	Important	No	No	2
			CVE-2022-37997	Elevation of Privilege	Important	No	No	1
			CVE-2022-38043	Information Disclosure	Important	No	No	2
			CVE-2022-24504	Remote Code Execution	Critical	No	No	2
			CVE-2022-37977	Denial of Service	Important	No	No	2
			CVE-2022-38051	Elevation of Privilege	Important	No	No	1
			CVE-2022-38044			No	No	2
			CVE-2022-38026	Information Disclosure	Important	No	No	2
			CVE-2022-22035	Remote Code Execution	Critical	No	No	2
			CVE-2022-33645	Denial of Service	Important	No	No	2
			CVE-2022-37989	Elevation of Privilege	Important	No	No	1

			CVE-2022-38041	Denial of Service	Important	No	No	2
			CVE-2022-38031	Remote Code Execution	Important	No	No	2
			CVE-2022-38032	Security Feature Bypass	Important	No	No	2
			CVE-2022-33634	Remote Code Execution	Critical	No	No	2
			CVE-2022-37986	Elevation of Privilege	Important	No	No	2
5018454	高危	October 11, 2022—KB5018454 (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	CVE-2022-37982	Remote Code Execution	Important	No	No	2
			CVE-2022-38033	Information Disclosure	Important	No	No	2
			CVE-2022-37975	Elevation of Privilege	Important	No	No	2
			CVE-2022-38034	Elevation of Privilege	Important	No	No	2
			CVE-2022-37999	Elevation of Privilege	Important	No	No	2
			CVE-2022-37988	Elevation of Privilege	Important	No	No	2
			CVE-2022-38022	Elevation of Privilege	Important	No	No	2
			CVE-2022-35770	Spoofing	Important	No	No	2
			CVE-2022-37981	Denial of Service	Important	No	No	2
			CVE-2022-37987	Elevation of Privilege	Important	No	No	1
			CVE-2022-37991	Elevation of Privilege	Important	No	No	2
			CVE-2022-30198	Remote Code Execution	Critical	No	No	2

		ESU,Windows Server 2008 R2 Datacenter ESU,Windows Embedded Standard 7 ESU,Windows Embedded POSReady 7 ESU	CVE-2022-38038	Elevation of Privilege	Important	No	No	2
			CVE-2022-38042	Elevation of Privilege	Important	No	No	2
			CVE-2022-33635	Remote Code Execution	Important	No	No	2
			CVE-2022-38047	Remote Code Execution	Critical	No	No	2
			CVE-2022-37993	Elevation of Privilege	Important	No	No	2
			CVE-2022-37978	Security Feature Bypass	Important	No	No	2
			CVE-2022-38000	Remote Code Execution	Critical	No	No	2
			CVE-2022-37994	Elevation of Privilege	Important	No	No	2
			CVE-2022-41033	Elevation of Privilege	Important	No	Yes	0
			CVE-2022-41081	Remote Code Execution	Critical	No	No	2
			CVE-2022-38040	Remote Code Execution	Important	No	No	2
			CVE-2022-37976	Elevation of Privilege	Critical	No	No	2
			CVE-2022-38037	Elevation of Privilege	Important	No	No	2
			CVE-2022-37990	Elevation of Privilege	Important	No	No	2
			CVE-2022-38029	Elevation of Privilege	Important	No	No	2
			CVE-2022-38043	Information Disclosure	Important	No	No	2

			CVE-2022-37985	Information Disclosure	Important	No	No	2
			CVE-2022-37997	Elevation of Privilege	Important	No	No	1
			CVE-2022-24504	Remote Code Execution	Critical	No	No	2
			CVE-2022-37977	Denial of Service	Important	No	No	2
			CVE-2022-38051	Elevation of Privilege	Important	No	No	1
			CVE-2022-38044			No	No	2
			CVE-2022-38026	Information Disclosure	Important	No	No	2
			CVE-2022-33645	Denial of Service	Important	No	No	2
			CVE-2022-22035	Remote Code Execution	Critical	No	No	2
			CVE-2022-37989	Elevation of Privilege	Important	No	No	1
			CVE-2022-38041	Denial of Service	Important	No	No	2
			CVE-2022-38031	Remote Code Execution	Important	No	No	2
			CVE-2022-38032	Security Feature Bypass	Important	No	No	2
			CVE-2022-33634	Remote Code Execution	Critical	No	No	2
			CVE-2022-37986	Elevation of Privilege	Important	No	No	2
5018425	高危	October 11, 2022—KB5018425 (OS Build 10240.19	CVE-2022-37982	Remote Code Execution	Important	No	No	2
			CVE-2022-38027	Elevation of Privilege	Important	No	No	2
			CVE-2022-38033	Information Disclosure	Important	No	No	2

		507) for Windows 10	CVE-2022-37975	Elevation of Privilege	Important	No	No	2
			CVE-2022-38034	Elevation of Privilege	Important	No	No	2
			CVE-2022-37999	Elevation of Privilege	Important	No	No	2
			CVE-2022-37988	Elevation of Privilege	Important	No	No	2
			CVE-2022-38022	Elevation of Privilege	Important	No	No	2
			CVE-2022-35770	Spoofing	Important	No	No	2
			CVE-2022-37984	Elevation of Privilege	Important	No	No	2
			CVE-2022-37981	Denial of Service	Important	No	No	2
			CVE-2022-37996	Information Disclosure	Important	No	No	2
			CVE-2022-37987	Elevation of Privilege	Important	No	No	1
			CVE-2022-37991	Elevation of Privilege	Important	No	No	2
			CVE-2022-30198	Remote Code Execution	Critical	No	No	2
			CVE-2022-38038	Elevation of Privilege	Important	No	No	2
			CVE-2022-38042	Elevation of Privilege	Important	No	No	2
			CVE-2022-38047	Remote Code Execution	Critical	No	No	2
			CVE-2022-37993	Elevation of Privilege	Important	No	No	2

			CVE-2022-37978	Security Feature Bypass	Important	No	No	2
			CVE-2022-38000	Remote Code Execution	Critical	No	No	2
			CVE-2022-37994	Elevation of Privilege	Important	No	No	2
			CVE-2022-37965	Denial of Service	Important	No	No	2
			CVE-2022-41033	Elevation of Privilege	Important	No	Yes	0
			CVE-2022-41081	Remote Code Execution	Critical	No	No	2
			CVE-2022-38040	Remote Code Execution	Important	No	No	2
			CVE-2022-38045	Elevation of Privilege	Important	No	No	2
			CVE-2022-38028	Elevation of Privilege	Important	No	No	1
			CVE-2022-38037	Elevation of Privilege	Important	No	No	2
			CVE-2022-37990	Elevation of Privilege	Important	No	No	2
			CVE-2022-38029	Elevation of Privilege	Important	No	No	2
			CVE-2022-37985	Information Disclosure	Important	No	No	2
			CVE-2022-38043	Information Disclosure	Important	No	No	2
			CVE-2022-37997	Elevation of Privilege	Important	No	No	1
			CVE-2022-24504	Remote Code Execution	Critical	No	No	2

			CVE-2022-37977	Denial of Service	Important	No	No	2
			CVE-2022-38051	Elevation of Privilege	Important	No	No	1
			CVE-2022-38044			No	No	2
			CVE-2022-38026	Information Disclosure	Important	No	No	2
			CVE-2022-22035	Remote Code Execution	Critical	No	No	2
			CVE-2022-33645	Denial of Service	Important	No	No	2
			CVE-2022-37989	Elevation of Privilege	Important	No	No	1
			CVE-2022-38041	Denial of Service	Important	No	No	2
			CVE-2022-33634	Remote Code Execution	Critical	No	No	2
			CVE-2022-38031	Remote Code Execution	Important	No	No	2
			CVE-2022-38032	Security Feature Bypass	Important	No	No	2
			CVE-2022-33635	Remote Code Execution	Important	No	No	2
			CVE-2022-37986	Elevation of Privilege	Important	No	No	2
5018446	高危	October 11, 2022—KB5018446 (Security-only update) for Windows Server 2008 Datacent	CVE-2022-37982	Remote Code Execution	Important	No	No	2
			CVE-2022-38033	Information Disclosure	Important	No	No	2
			CVE-2022-37975	Elevation of Privilege	Important	No	No	2
			CVE-2022-38034	Elevation of Privilege	Important	No	No	2
			CVE-2022-37999	Elevation of Privilege	Important	No	No	2

		er ESU,Windows Server 2008 Standard ESU,Windows Server 2008 Enterprise ESU	CVE-2022-37988	Elevation of Privilege	Important	No	No	2
			CVE-2022-35770	Spoofing	Important	No	No	2
			CVE-2022-37981	Denial of Service	Important	No	No	2
			CVE-2022-37987	Elevation of Privilege	Important	No	No	1
			CVE-2022-37991	Elevation of Privilege	Important	No	No	2
			CVE-2022-38042	Elevation of Privilege	Important	No	No	2
			CVE-2022-38047	Remote Code Execution	Critical	No	No	2
			CVE-2022-37993	Elevation of Privilege	Important	No	No	2
			CVE-2022-37978	Security Feature Bypass	Important	No	No	2
			CVE-2022-37994	Elevation of Privilege	Important	No	No	2
			CVE-2022-41033	Elevation of Privilege	Important	No	Yes	0
			CVE-2022-41081	Remote Code Execution	Critical	No	No	2
			CVE-2022-38040	Remote Code Execution	Important	No	No	2
			CVE-2022-37976	Elevation of Privilege	Critical	No	No	2
			CVE-2022-37986	Elevation of Privilege	Important	No	No	2
			CVE-2022-38037	Elevation of Privilege	Important	No	No	2

			CVE-2022-37990	Elevation of Privilege	Important	No	No	2
			CVE-2022-38029	Elevation of Privilege	Important	No	No	2
			CVE-2022-37985	Information Disclosure	Important	No	No	2
			CVE-2022-37997	Elevation of Privilege	Important	No	No	1
			CVE-2022-24504	Remote Code Execution	Critical	No	No	2
			CVE-2022-37977	Denial of Service	Important	No	No	2
			CVE-2022-38051	Elevation of Privilege	Important	No	No	1
			CVE-2022-38044			No	No	2
			CVE-2022-33645	Denial of Service	Important	No	No	2
			CVE-2022-37989	Elevation of Privilege	Important	No	No	1
			CVE-2022-33634	Remote Code Execution	Critical	No	No	2
			CVE-2022-38031	Remote Code Execution	Important	No	No	2
			CVE-2022-38032	Security Feature Bypass	Important	No	No	2
			CVE-2022-33635	Remote Code Execution	Important	No	No	2
			CVE-2022-38038	Elevation of Privilege	Important	No	No	2
5018479	高危	October 11, 2022—KB501847	CVE-2022-37982	Remote Code Execution	Important	No	No	2
			CVE-2022-38033	Information Disclosure	Important	No	No	2

		9 (Security-only update) 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 ESU,Windows Embedded Standard 7 ESU,Windows Embedded	CVE-2022-37975	Elevation of Privilege	Important	No	No	2
			CVE-2022-38034	Elevation of Privilege	Important	No	No	2
			CVE-2022-37999	Elevation of Privilege	Important	No	No	2
			CVE-2022-37988	Elevation of Privilege	Important	No	No	2
			CVE-2022-38022	Elevation of Privilege	Important	No	No	2
			CVE-2022-35770	Spoofing	Important	No	No	2
			CVE-2022-37981	Denial of Service	Important	No	No	2
			CVE-2022-37987	Elevation of Privilege	Important	No	No	1
			CVE-2022-37991	Elevation of Privilege	Important	No	No	2
			CVE-2022-30198	Remote Code Execution	Critical	No	No	2
			CVE-2022-38038	Elevation of Privilege	Important	No	No	2
			CVE-2022-38042	Elevation of Privilege	Important	No	No	2
			CVE-2022-33635	Remote Code Execution	Important	No	No	2
			CVE-2022-38047	Remote Code Execution	Critical	No	No	2
			CVE-2022-37993	Elevation of Privilege	Important	No	No	2
			CVE-2022-37978	Security Feature Bypass	Important	No	No	2

		POSReady 7 ESU	CVE-2022-38000	Remote Code Execution	Critical	No	No	2
			CVE-2022-37994	Elevation of Privilege	Important	No	No	2
			CVE-2022-41033	Elevation of Privilege	Important	No	Yes	0
			CVE-2022-41081	Remote Code Execution	Critical	No	No	2
			CVE-2022-38040	Remote Code Execution	Important	No	No	2
			CVE-2022-37976	Elevation of Privilege	Critical	No	No	2
			CVE-2022-38037	Elevation of Privilege	Important	No	No	2
			CVE-2022-37990	Elevation of Privilege	Important	No	No	2
			CVE-2022-38029	Elevation of Privilege	Important	No	No	2
			CVE-2022-38043	Information Disclosure	Important	No	No	2
			CVE-2022-37985	Information Disclosure	Important	No	No	2
			CVE-2022-37997	Elevation of Privilege	Important	No	No	1
			CVE-2022-24504	Remote Code Execution	Critical	No	No	2
			CVE-2022-37977	Denial of Service	Important	No	No	2
			CVE-2022-38051	Elevation of Privilege	Important	No	No	1
			CVE-2022-38044			No	No	2
			CVE-2022-38026	Information Disclosure	Important	No	No	2

			CVE-2022-33645	Denial of Service	Important	No	No	2
			CVE-2022-22035	Remote Code Execution	Critical	No	No	2
			CVE-2022-37989	Elevation of Privilege	Important	No	No	1
			CVE-2022-38041	Denial of Service	Important	No	No	2
			CVE-2022-38031	Remote Code Execution	Important	No	No	2
			CVE-2022-38032	Security Feature Bypass	Important	No	No	2
			CVE-2022-33634	Remote Code Execution	Critical	No	No	2
			CVE-2022-37986	Elevation of Privilege	Important	No	No	2
5018450	高危	October 11, 2022—KB5018450 (Monthly Rollup) for Windows Server 2008 Datacenter ESU,Windows Server 2008 Standard ESU,Windows Server 2008	CVE-2022-37982	Remote Code Execution	Important	No	No	2
			CVE-2022-38033	Information Disclosure	Important	No	No	2
			CVE-2022-37975	Elevation of Privilege	Important	No	No	2
			CVE-2022-38034	Elevation of Privilege	Important	No	No	2
			CVE-2022-37999	Elevation of Privilege	Important	No	No	2
			CVE-2022-37988	Elevation of Privilege	Important	No	No	2
			CVE-2022-35770	Spoofing	Important	No	No	2
			CVE-2022-37981	Denial of Service	Important	No	No	2
			CVE-2022-37987	Elevation of Privilege	Important	No	No	1

		Enterprise ESU	CVE-2022-37991	Elevation of Privilege	Important	No	No	2
			CVE-2022-38042	Elevation of Privilege	Important	No	No	2
			CVE-2022-38047	Remote Code Execution	Critical	No	No	2
			CVE-2022-37993	Elevation of Privilege	Important	No	No	2
			CVE-2022-37978	Security Feature Bypass	Important	No	No	2
			CVE-2022-37994	Elevation of Privilege	Important	No	No	2
			CVE-2022-41033	Elevation of Privilege	Important	No	Yes	0
			CVE-2022-41081	Remote Code Execution	Critical	No	No	2
			CVE-2022-38040	Remote Code Execution	Important	No	No	2
			CVE-2022-37976	Elevation of Privilege	Critical	No	No	2
			CVE-2022-37986	Elevation of Privilege	Important	No	No	2
			CVE-2022-38037	Elevation of Privilege	Important	No	No	2
			CVE-2022-37990	Elevation of Privilege	Important	No	No	2
			CVE-2022-38029	Elevation of Privilege	Important	No	No	2
			CVE-2022-37985	Information Disclosure	Important	No	No	2

			CVE-2022-37997	Elevation of Privilege	Important	No	No	1
			CVE-2022-24504	Remote Code Execution	Critical	No	No	2
			CVE-2022-37977	Denial of Service	Important	No	No	2
			CVE-2022-38051	Elevation of Privilege	Important	No	No	1
			CVE-2022-38044			No	No	2
			CVE-2022-33645	Denial of Service	Important	No	No	2
			CVE-2022-37989	Elevation of Privilege	Important	No	No	1
			CVE-2022-33634	Remote Code Execution	Critical	No	No	2
			CVE-2022-38031	Remote Code Execution	Important	No	No	2
			CVE-2022-38032	Security Feature Bypass	Important	No	No	2
			CVE-2022-33635	Remote Code Execution	Important	No	No	2
			CVE-2022-38038	Elevation of Privilege	Important	No	No	2
5018411	高危	October 11, 2022—KB5018411 (OS Build 14393.5427) for Windows 10, version 1607, all	CVE-2022-37982	Remote Code Execution	Important	No	No	2
			CVE-2022-38027	Elevation of Privilege	Important	No	No	2
			CVE-2022-38033	Information Disclosure	Important	No	No	2
			CVE-2022-37975	Elevation of Privilege	Important	No	No	2
			CVE-2022-38034	Elevation of Privilege	Important	No	No	2

		editions,Windows Server 2016, all editions	CVE-2022-37999	Elevation of Privilege	Important	No	No	2
			CVE-2022-37988	Elevation of Privilege	Important	No	No	2
			CVE-2022-38022	Elevation of Privilege	Important	No	No	2
			CVE-2022-37984	Elevation of Privilege	Important	No	No	2
			CVE-2022-35770	Spoofing	Important	No	No	2
			CVE-2022-37981	Denial of Service	Important	No	No	2
			CVE-2022-37996	Information Disclosure	Important	No	No	2
			CVE-2022-37987	Elevation of Privilege	Important	No	No	1
			CVE-2022-37991	Elevation of Privilege	Important	No	No	2
			CVE-2022-30198	Remote Code Execution	Critical	No	No	2
			CVE-2022-38038	Elevation of Privilege	Important	No	No	2
			CVE-2022-38042	Elevation of Privilege	Important	No	No	2
			CVE-2022-38047	Remote Code Execution	Critical	No	No	2
			CVE-2022-37993	Elevation of Privilege	Important	No	No	2
			CVE-2022-37978	Security Feature Bypass	Important	No	No	2
			CVE-2022-38003	Elevation of Privilege	Important	No	No	2

			CVE-2022-38000	Remote Code Execution	Critical	No	No	2
			CVE-2022-37994	Elevation of Privilege	Important	No	No	2
			CVE-2022-37965	Denial of Service	Important	No	No	2
			CVE-2022-41033	Elevation of Privilege	Important	No	Yes	0
			CVE-2022-41081	Remote Code Execution	Critical	No	No	2
			CVE-2022-38040	Remote Code Execution	Important	No	No	2
			CVE-2022-38045	Elevation of Privilege	Important	No	No	2
			CVE-2022-37976	Elevation of Privilege	Critical	No	No	2
			CVE-2022-38028	Elevation of Privilege	Important	No	No	1
			CVE-2022-38037	Elevation of Privilege	Important	No	No	2
			CVE-2022-37990	Elevation of Privilege	Important	No	No	2
			CVE-2022-38029	Elevation of Privilege	Important	No	No	2
			CVE-2022-38021	Elevation of Privilege	Important	No	No	2
			CVE-2022-38043	Information Disclosure	Important	No	No	2
			CVE-2022-37997	Elevation of Privilege	Important	No	No	1
			CVE-2022-37985	Information Disclosure	Important	No	No	2

			CVE-2022-24504	Remote Code Execution	Critical	No	No	2
			CVE-2022-37977	Denial of Service	Important	No	No	2
			CVE-2022-38051	Elevation of Privilege	Important	No	No	1
			CVE-2022-38044			No	No	2
			CVE-2022-38026	Information Disclosure	Important	No	No	2
			CVE-2022-37979	Elevation of Privilege	Critical	No	No	2
			CVE-2022-22035	Remote Code Execution	Critical	No	No	2
			CVE-2022-33645	Denial of Service	Important	No	No	2
			CVE-2022-37989	Elevation of Privilege	Important	No	No	1
			CVE-2022-38041	Denial of Service	Important	No	No	2
			CVE-2022-33634	Remote Code Execution	Critical	No	No	2
			CVE-2022-38031	Remote Code Execution	Important	No	No	2
			CVE-2022-37995	Elevation of Privilege	Important	No	No	2
			CVE-2022-38032	Security Feature Bypass	Important	No	No	2
			CVE-2022-33635	Remote Code Execution	Important	No	No	2
			CVE-2022-37986	Elevation of Privilege	Important	No	No	2
5018418	高危	October 11, 2022—KB5018418 (OS	CVE-2022-37982	Remote Code Execution	Important	No	No	2
			CVE-2022-38027	Elevation of Privilege	Important	No	No	2

		Build 22000.1098) for Windows 11 version 21H2, all editions	CVE-2022-38033	Information Disclosure	Important	No	No	2
			CVE-2022-37975	Elevation of Privilege	Important	No	No	2
			CVE-2022-38034	Elevation of Privilege	Important	No	No	2
			CVE-2022-37999	Elevation of Privilege	Important	No	No	2
			CVE-2022-37988	Elevation of Privilege	Important	No	No	2
			CVE-2022-38022	Elevation of Privilege	Important	No	No	2
			CVE-2022-37984	Elevation of Privilege	Important	No	No	2
			CVE-2022-35770	Spoofing	Important	No	No	2
			CVE-2022-38025	Information Disclosure	Important	No	No	2
			CVE-2022-37981	Denial of Service	Important	No	No	2
			CVE-2022-37996	Information Disclosure	Important	No	No	2
			CVE-2022-37987	Elevation of Privilege	Important	No	No	1
			CVE-2022-37991	Elevation of Privilege	Important	No	No	2
			CVE-2022-30198	Remote Code Execution	Critical	No	No	2
			CVE-2022-38038	Elevation of Privilege	Important	No	No	2
			CVE-2022-38042	Elevation of Privilege	Important	No	No	2

			CVE-2022-33635	Remote Code Execution	Important	No	No	2
			CVE-2022-38047	Remote Code Execution	Critical	No	No	2
			CVE-2022-37993	Elevation of Privilege	Important	No	No	2
			CVE-2022-38046	Information Disclosure	Important	No	No	2
			CVE-2022-37970	Elevation of Privilege	Important	No	No	1
			CVE-2022-38016	Elevation of Privilege	Important	No	No	2
			CVE-2022-37978	Security Feature Bypass	Important	No	No	2
			CVE-2022-38039	Elevation of Privilege	Important	No	No	2
			CVE-2022-38003	Elevation of Privilege	Important	No	No	2
			CVE-2022-38050	Elevation of Privilege	Important	No	No	1
			CVE-2022-37994	Elevation of Privilege	Important	No	No	2
			CVE-2022-37983	Elevation of Privilege	Important	No	No	2
			CVE-2022-37998	Denial of Service	Important	No	No	2
			CVE-2022-37965	Denial of Service	Important	No	No	2
			CVE-2022-41033	Elevation of Privilege	Important	No	Yes	0
			CVE-2022-38000	Remote Code Execution	Critical	No	No	2

			CVE-2022-37973	Denial of Service	Important	No	No	2
			CVE-2022-41081	Remote Code Execution	Critical	No	No	2
			CVE-2022-38040	Remote Code Execution	Important	No	No	2
			CVE-2022-38045	Elevation of Privilege	Important	No	No	2
			CVE-2022-38028	Elevation of Privilege	Important	No	No	1
			CVE-2022-38037	Elevation of Privilege	Important	No	No	2
			CVE-2022-37990	Elevation of Privilege	Important	No	No	2
			CVE-2022-38029	Elevation of Privilege	Important	No	No	2
			CVE-2022-37980	Elevation of Privilege	Important	No	No	2
			CVE-2022-38021	Elevation of Privilege	Important	No	No	2
			CVE-2022-37985	Information Disclosure	Important	No	No	2
			CVE-2022-38043	Information Disclosure	Important	No	No	2
			CVE-2022-37997	Elevation of Privilege	Important	No	No	1
			CVE-2022-38036	Denial of Service	Important	No	No	2
			CVE-2022-24504	Remote Code Execution	Critical	No	No	2
			CVE-2022-37977	Denial of Service	Important	No	No	2
			CVE-2022-37974	Information Disclosure	Important	No	No	1

			CVE-2022-38051	Elevation of Privilege	Important	No	No	1
			CVE-2022-38044			No	No	2
			CVE-2022-38026	Information Disclosure	Important	No	No	2
			CVE-2022-37979	Elevation of Privilege	Critical	No	No	2
			CVE-2022-22035	Remote Code Execution	Critical	No	No	2
			CVE-2022-33645	Denial of Service	Important	No	No	2
			CVE-2022-37989	Elevation of Privilege	Important	No	No	1
			CVE-2022-38041	Denial of Service	Important	No	No	2
			CVE-2022-38030	Information Disclosure	Important	No	No	2
			CVE-2022-38031	Remote Code Execution	Important	No	No	2
			CVE-2022-37995	Elevation of Privilege	Important	No	No	2
			CVE-2022-38032	Security Feature Bypass	Important	No	No	2
			CVE-2022-33634	Remote Code Execution	Critical	No	No	2
			CVE-2022-37986	Elevation of Privilege	Important	No	No	2
5018474	高危	October 11, 2022—KB5018474 (Monthly Rollup)	CVE-2022-37982	Remote Code Execution	Important	No	No	2
			CVE-2022-38027	Elevation of Privilege	Important	No	No	2
			CVE-2022-38033	Information Disclosure	Important	No	No	2

		for Windows 8.1,Windows RT 8.1,Windows Server 2012 R2,Windows Embedded 8.1 Industry Enterprise,Windows Embedded 8.1 Industry Pro	CVE-2022-37975	Elevation of Privilege	Important	No	No	2
			CVE-2022-38034	Elevation of Privilege	Important	No	No	2
			CVE-2022-37999	Elevation of Privilege	Important	No	No	2
			CVE-2022-37988	Elevation of Privilege	Important	No	No	2
			CVE-2022-38022	Elevation of Privilege	Important	No	No	2
			CVE-2022-37984	Elevation of Privilege	Important	No	No	2
			CVE-2022-35770	Spoofing	Important	No	No	2
			CVE-2022-37981	Denial of Service	Important	No	No	2
			CVE-2022-37996	Information Disclosure	Important	No	No	2
			CVE-2022-37987	Elevation of Privilege	Important	No	No	1
			CVE-2022-37991	Elevation of Privilege	Important	No	No	2
			CVE-2022-30198	Remote Code Execution	Critical	No	No	2
			CVE-2022-38038	Elevation of Privilege	Important	No	No	2
			CVE-2022-38042	Elevation of Privilege	Important	No	No	2
			CVE-2022-38047	Remote Code Execution	Critical	No	No	2
			CVE-2022-37993	Elevation of Privilege	Important	No	No	2

			CVE-2022-37978	Security Feature Bypass	Important	No	No	2
			CVE-2022-38000	Remote Code Execution	Critical	No	No	2
			CVE-2022-37994	Elevation of Privilege	Important	No	No	2
			CVE-2022-37965	Denial of Service	Important	No	No	2
			CVE-2022-41033	Elevation of Privilege	Important	No	Yes	0
			CVE-2022-41081	Remote Code Execution	Critical	No	No	2
			CVE-2022-38040	Remote Code Execution	Important	No	No	2
			CVE-2022-38045	Elevation of Privilege	Important	No	No	2
			CVE-2022-37976	Elevation of Privilege	Critical	No	No	2
			CVE-2022-38028	Elevation of Privilege	Important	No	No	1
			CVE-2022-38037	Elevation of Privilege	Important	No	No	2
			CVE-2022-37990	Elevation of Privilege	Important	No	No	2
			CVE-2022-38029	Elevation of Privilege	Important	No	No	2
			CVE-2022-37985	Information Disclosure	Important	No	No	2
			CVE-2022-37997	Elevation of Privilege	Important	No	No	1
			CVE-2022-38043	Information Disclosure	Important	No	No	2

			CVE-2022-24504	Remote Code Execution	Critical	No	No	2
			CVE-2022-37977	Denial of Service	Important	No	No	2
			CVE-2022-38051	Elevation of Privilege	Important	No	No	1
			CVE-2022-38044			No	No	2
			CVE-2022-38026	Information Disclosure	Important	No	No	2
			CVE-2022-22035	Remote Code Execution	Critical	No	No	2
			CVE-2022-33645	Denial of Service	Important	No	No	2
			CVE-2022-37989	Elevation of Privilege	Important	No	No	1
			CVE-2022-38041	Denial of Service	Important	No	No	2
			CVE-2022-33634	Remote Code Execution	Critical	No	No	2
			CVE-2022-38031	Remote Code Execution	Important	No	No	2
			CVE-2022-38032	Security Feature Bypass	Important	No	No	2
			CVE-2022-33635	Remote Code Execution	Important	No	No	2
			CVE-2022-37986	Elevation of Privilege	Important	No	No	2
5018476	高危	October 11, 2022—KB5018476 (Security-only update) for Windows	CVE-2022-37982	Remote Code Execution	Important	No	No	2
			CVE-2022-38027	Elevation of Privilege	Important	No	No	2
			CVE-2022-38033	Information Disclosure	Important	No	No	2
			CVE-2022-37975	Elevation of Privilege	Important	No	No	2

		8.1,Windows RT 8.1,Windows Server 2012 R2,Windows Embedded 8.1 Industry Enterprise,Windows Embedded 8.1 Industry Pro	CVE-2022-38034	Elevation of Privilege	Important	No	No	2
			CVE-2022-37999	Elevation of Privilege	Important	No	No	2
			CVE-2022-37988	Elevation of Privilege	Important	No	No	2
			CVE-2022-38022	Elevation of Privilege	Important	No	No	2
			CVE-2022-37984	Elevation of Privilege	Important	No	No	2
			CVE-2022-35770	Spoofing	Important	No	No	2
			CVE-2022-37981	Denial of Service	Important	No	No	2
			CVE-2022-37996	Information Disclosure	Important	No	No	2
			CVE-2022-37987	Elevation of Privilege	Important	No	No	1
			CVE-2022-37991	Elevation of Privilege	Important	No	No	2
			CVE-2022-30198	Remote Code Execution	Critical	No	No	2
			CVE-2022-38038	Elevation of Privilege	Important	No	No	2
			CVE-2022-38042	Elevation of Privilege	Important	No	No	2
			CVE-2022-38047	Remote Code Execution	Critical	No	No	2
			CVE-2022-37993	Elevation of Privilege	Important	No	No	2
			CVE-2022-37978	Security Feature Bypass	Important	No	No	2

			CVE-2022-38000	Remote Code Execution	Critical	No	No	2
			CVE-2022-37994	Elevation of Privilege	Important	No	No	2
			CVE-2022-37965	Denial of Service	Important	No	No	2
			CVE-2022-41033	Elevation of Privilege	Important	No	Yes	0
			CVE-2022-41081	Remote Code Execution	Critical	No	No	2
			CVE-2022-38040	Remote Code Execution	Important	No	No	2
			CVE-2022-38045	Elevation of Privilege	Important	No	No	2
			CVE-2022-37976	Elevation of Privilege	Critical	No	No	2
			CVE-2022-38028	Elevation of Privilege	Important	No	No	1
			CVE-2022-38037	Elevation of Privilege	Important	No	No	2
			CVE-2022-37990	Elevation of Privilege	Important	No	No	2
			CVE-2022-38029	Elevation of Privilege	Important	No	No	2
			CVE-2022-37985	Information Disclosure	Important	No	No	2
			CVE-2022-37997	Elevation of Privilege	Important	No	No	1
			CVE-2022-38043	Information Disclosure	Important	No	No	2
			CVE-2022-24504	Remote Code Execution	Critical	No	No	2

			CVE-2022-37977	Denial of Service	Important	No	No	2
			CVE-2022-38051	Elevation of Privilege	Important	No	No	1
			CVE-2022-38044			No	No	2
			CVE-2022-38026	Information Disclosure	Important	No	No	2
			CVE-2022-22035	Remote Code Execution	Critical	No	No	2
			CVE-2022-33645	Denial of Service	Important	No	No	2
			CVE-2022-37989	Elevation of Privilege	Important	No	No	1
			CVE-2022-38041	Denial of Service	Important	No	No	2
			CVE-2022-33634	Remote Code Execution	Critical	No	No	2
			CVE-2022-38031	Remote Code Execution	Important	No	No	2
			CVE-2022-38032	Security Feature Bypass	Important	No	No	2
			CVE-2022-33635	Remote Code Execution	Important	No	No	2
			CVE-2022-37986	Elevation of Privilege	Important	No	No	2

本月微软发布的软件安全更新补丁共 5 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
5002279	高危	Description of the security update for Office 2013: October 11, 2022 (KB5002279)	CVE-2022-38048	Remote Code Execution	Critical	No	No	2
5002026	高危	Description of the security update for Office 2016: October 11, 2022 (KB5002026)	CVE-2022-38048	Remote Code Execution	Critical	No	No	2
5002287	高危	Description of the security update for SharePoint Enterprise Server 2016: October 11, 2022 (KB5002287)	CVE-2022-41037	Remote Code Execution	Important	No	No	2
			CVE-2022-38053	Remote Code Execution	Important	No	No	1
			CVE-2022-41036	Remote Code Execution	Important	No	No	1

			CVE-2022-41038	Remote Code Execution	Critical	No	No	1
5002284	高危	Description of the security update for SharePoint Foundation 2013: October 11, 2022 (KB5002284)	CVE-2022-41037	Remote Code Execution	Important	No	No	2
			CVE-2022-38053	Remote Code Execution	Important	No	No	1
			CVE-2022-41036	Remote Code Execution	Important	No	No	1
			CVE-2022-41038	Remote Code Execution	Critical	No	No	1
5002288	高危	Description of the security update for Office 2016: October 11, 2022 (KB5002288)	CVE-2022-38048	Remote Code Execution	Critical	No	No	2

本月发布内容中还包括 2 个一般性更新补丁：

KBID	奇安信集团级别	详细信息
5002243	其他功能性补丁	Office 2016 更新程序
5002274	其他功能性补丁	Office 2013 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