奇安信集团 2022 年 11 月补丁库

更新通告

第一次更新

奇安信集团漏洞补丁运营团队

2022 年 11 月 09 日

目 录

文档信息

文档名称	奇安信集团 2022 年 11 月补丁库更新通告		
文档编号	Qi An Xin Group-MSPatch-2022-1101		
发布日期	2022-11-09	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:2022.11.09.1,V10版本:2022.11.09.1000)已发布，本次更新推送了42个微软安全补丁，修复了55个安全漏洞，其中9个微软官方评级为“严重(Critical)”，46个评级为“重要(Important)”，这些漏洞影响产品Windows、Microsoft Office和.NET Framework。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 23 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
5020003 5020005 5020000 5020010 5020019 5019961 5020023 5019980 5020013 5019959 5020009 5019964 5019970 5019966	CVE-2022-41057	Elevation of Privilege	Important	No	No	Exploitation More Likely
5020003 5020000 5020010 5019961 5020023 5019980 5020013 5019959 5020009 5019964 5019970 5019966 5019958	CVE-2022-41128	Remote Code Execution	Critical	No	Yes	Exploitation Detected

5020003 5020000 5020010 5019961 5020023 5019980 5020013 5019959 5020009 5019964 5019970 5019966	CVE-2022-41090	Denial of Service	Important	No	No	Exploitation More Likely
5020003 5020005 5020000 5020010 5020019 5019961 5020023 5019980 5020013 5019959 5020009 5019964 5019970 5019966	CVE-2022-41073	Elevation of Privilege	Important	No	Yes	Exploitation Detected
5020003 5020005 5020000 5020010 5020019 5020023 5020013 5020009 5019964 5019966	CVE-2022-38023	Elevation of Privilege	Important	No	No	Exploitation More Likely
5020003 5020005 5020000 5020010 5020019	CVE-2022-37966	Elevation of Privilege	Critical	No	No	Exploitation More Likely

5020023 5020013 5020009 5019964 5019966						
5020003 5020010 5019961 5020023 5019980 5019959 5020009 5019964 5019970 5019966	CVE-2022-41125	Elevation of Privilege	Important	No	Yes	Exploitation Detected
5020003 5020005 5020000 5020010 5020019 5019961 5020023 5019980 5020013 5019959 5020009 5019964 5019970 5019966	CVE-2022-41058	Denial of Service	Important	No	No	Exploitation More Likely
5020003 5020000 5020010 5019961 5020023 5019980 5020013 5019959 5020009 5019964 5019970 5019966	CVE-2022-41039	Remote Code Execution	Critical	No	No	Exploitation Less Likely

5020003 5020005 5020000 5020010 5020019 5019961 5020023 5019980 5020013 5019959 5020009 5019964 5019970 5019966	CVE-2022-41109	Elevation of Privilege	Important	No	No	Exploitation More Likely
5020003 5020005 5020000 5020010 5020019 5020023 5020013 5020009 5019964 5019966	CVE-2022-37967	Elevation of Privilege	Critical	No	No	Exploitation More Likely
5020005 5020000 5020019 5020013	CVE-2022-41044	Remote Code Execution	Critical	No	No	Exploitation Less Likely
5020000 5020010 5019961 5020023 5019980 5020013 5019959 5019964 5019970 5019966 5019958	CVE-2022-41118	Remote Code Execution	Critical	No	No	Exploitation More Likely
5019758	CVE-2022-41123	Elevation	Important	No	No	Exploitation

		of Privilege				More Likely
5019758	CVE-2022-41080	Elevation of Privilege	Critical	No	No	Exploitation More Likely
5019758	CVE-2022-41079	Spoofing	Important	No	No	Exploitation More Likely
5019961 5019980 5019959 5019964 5019970 5019966	CVE-2022-38015	Denial of Service	Critical	No	No	Exploitation Less Likely
5019961 5019980 5019959 5019966	CVE-2022-41113	Elevation of Privilege	Important	No	No	Exploitation More Likely
5019961 5019980 5019959 5019966	CVE-2022-41055	Information Disclosure	Important	No	No	Exploitation More Likely
5019961 5019980 5019959	CVE-2022-41092	Elevation of Privilege	Important	No	No	Exploitation More Likely
5019961 5019980 5019959 5019964 5019970 5019966	CVE-2022-41049	Security Feature Bypass	Important	No	No	Exploitation More Likely
5019961 5019980 5019959 5019964 5019970	CVE-2022-41091	Security Feature Bypass	Important	Yes	Yes	Exploitation Detected

5019966						
5019961 5019980 5019959 5019966	CVE-2022-41096	Elevation of Privilege	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 30 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
5020003	高危	November 8, 2022 — KB5020003 (Security-only update) for Windows Server 2012, Windows Embedded 8 Standard	CVE-2022-23824	Information Disclosure	Important	No	No	2
			CVE-2022-41057	Elevation of Privilege	Important	No	No	1
			CVE-2022-41053	Denial of Service	Important	No	No	2
			CVE-2022-41128	Remote Code Execution	Critical	No	Yes	0
			CVE-2022-37992	Elevation of Privilege	Important	No	No	2
			CVE-2022-41097	Information Disclosure	Important	No	No	2
			CVE-2022-41090	Denial of Service	Important	No	No	1
			CVE-2022-41073	Elevation of Privilege	Important	No	Yes	0
			CVE-2022-41048	Remote Code Execution	Important	No	No	2
			CVE-2022-38023	Elevation of Privilege	Important	No	No	1

			CVE-2022-41045	Elevation of Privilege	Important	No	No	2
			CVE-2022-41095	Elevation of Privilege	Important	No	No	2
			CVE-2022-41047	Remote Code Execution	Important	No	No	2
			CVE-2022-37966	Elevation of Privilege	Critical	No	No	1
			CVE-2022-41086	Elevation of Privilege	Important	No	No	2
			CVE-2022-41125	Elevation of Privilege	Important	No	Yes	0
			CVE-2022-41088	Remote Code Execution	Critical	No	No	2
			CVE-2022-41058	Denial of Service	Important	No	No	1
			CVE-2022-41039	Remote Code Execution	Critical	No	No	2
			CVE-2022-41109	Elevation of Privilege	Important	No	No	1
			CVE-2022-41056	Denial of Service	Important	No	No	2
			CVE-2022-41098	Information Disclosure	Important	No	No	2
			CVE-2022-37967	Elevation of Privilege	Critical	No	No	1
5020005	高危	November 8,	CVE-2022-23824	Information Disclosure	Important	No	No	2

		2022 — KB5020005 (Security-only update) for Windows Server 2008 Datacenter ESU,Windows Server 2008 Standard ESU,Windows Server 2008 Enterprise ESU	CVE-2022-41057	Elevation of Privilege	Important	No	No	1
			CVE-2022-41053	Denial of Service	Important	No	No	2
			CVE-2022-37992	Elevation of Privilege	Important	No	No	2
			CVE-2022-41097	Information Disclosure	Important	No	No	2
			CVE-2022-41073	Elevation of Privilege	Important	No	Yes	0
			CVE-2022-41048	Remote Code Execution	Important	No	No	2
			CVE-2022-38023	Elevation of Privilege	Important	No	No	1
			CVE-2022-41045	Elevation of Privilege	Important	No	No	2
			CVE-2022-41095	Elevation of Privilege	Important	No	No	2
			CVE-2022-41047	Remote Code Execution	Important	No	No	2
			CVE-2022-37966	Elevation of Privilege	Critical	No	No	1
			CVE-2022-41086	Elevation of Privilege	Important	No	No	2
			CVE-2022-41058	Denial of Service	Important	No	No	1
			CVE-2022-41109	Elevation of Privilege	Important	No	No	1

			CVE-2022-41056	Denial of Service	Important	No	No	2
			CVE-2022-41098	Information Disclosure	Important	No	No	2
			CVE-2022-41044	Remote Code Execution	Critical	No	No	2
			CVE-2022-37967	Elevation of Privilege	Critical	No	No	1
5020000	高危	November 8, 2022 — KB5020000 (Monthly Rollup) for Windows 7 Enterprise ESU,Windows 7 Professional ESU,Windows 7 Ultimate ESU,Wind	CVE-2022-41116	Denial of Service	Important	No	No	2
			CVE-2022-23824	Information Disclosure	Important	No	No	2
			CVE-2022-41057	Elevation of Privilege	Important	No	No	1
			CVE-2022-41053	Denial of Service	Important	No	No	2
			CVE-2022-41128	Remote Code Execution	Critical	No	Yes	0
			CVE-2022-37992	Elevation of Privilege	Important	No	No	2
			CVE-2022-41097	Information Disclosure	Important	No	No	2
			CVE-2022-41090	Denial of Service	Important	No	No	1
			CVE-2022-41073	Elevation of Privilege	Important	No	Yes	0
			CVE-2022-41048	Remote Code Execution	Important	No	No	2

		ows Server 2008 R2 Enterprise ESU,Windows Server 2008 R2 Standard ESU,Windows Server 2008 R2 Datacenter ESU,Windows Embedded Standard 7 ESU,Windows Embedded POSReady 7 ESU	CVE-2022-38023	Elevation of Privilege	Important	No	No	1
			CVE-2022-41118	Remote Code Execution	Critical	No	No	1
			CVE-2022-41045	Elevation of Privilege	Important	No	No	2
			CVE-2022-41095	Elevation of Privilege	Important	No	No	2
			CVE-2022-41047	Remote Code Execution	Important	No	No	2
			CVE-2022-37966	Elevation of Privilege	Critical	No	No	1
			CVE-2022-41086	Elevation of Privilege	Important	No	No	2
			CVE-2022-41058	Denial of Service	Important	No	No	1
			CVE-2022-41039	Remote Code Execution	Critical	No	No	2
			CVE-2022-41109	Elevation of Privilege	Important	No	No	1
			CVE-2022-41056	Denial of Service	Important	No	No	2
			CVE-2022-41098	Information Disclosure	Important	No	No	2
			CVE-2022-41044	Remote Code Execution	Critical	No	No	2
			CVE-2022-37967	Elevation of Privilege	Critical	No	No	1

5020679	高危	November 8, 2022-Security Only Update for .NET Framework 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Windows Server 2012 (KB5020679)	CVE-2022-41064	Information Disclosure	Important	No	No	2
5020694	高危	November 8, 2022-KB5020694 Cumulative Update for .NET Framework 3.5, 4.8 and	CVE-2022-41064	Information Disclosure	Important	No	No	2

		4.8.1 for Windows 10 Version 22H2						
5020010	高危	November 8, 2022 — KB5020010 (Security-only update) for Windows 8.1,Windows RT 8.1,Windows Server 2012 R2,Windows Embedded 8.1 Industry Enterpri	CVE-2022-23824	Information Disclosure	Important	No	No	2
			CVE-2022-41053	Denial of Service	Important	No	No	2
			CVE-2022-41093	Elevation of Privilege	Important	No	No	2
			CVE-2022-41128	Remote Code Execution	Critical	No	Yes	0
			CVE-2022-37992	Elevation of Privilege	Important	No	No	2
			CVE-2022-41097	Information Disclosure	Important	No	No	2
			CVE-2022-37967	Elevation of Privilege	Critical	No	No	1
			CVE-2022-41100	Elevation of Privilege	Important	No	No	2
			CVE-2022-41090	Denial of Service	Important	No	No	1
			CVE-2022-41073	Elevation of Privilege	Important	No	Yes	0
			CVE-2022-41048	Remote Code Execution	Important	No	No	2

		se,Windows Embedded 8.1 Industry Pro	CVE-2022-38023	Elevation of Privilege	Important	No	No	1
			CVE-2022-41118	Remote Code Execution	Critical	No	No	1
			CVE-2022-41045	Elevation of Privilege	Important	No	No	2
			CVE-2022-41095	Elevation of Privilege	Important	No	No	2
			CVE-2022-41047	Remote Code Execution	Important	No	No	2
			CVE-2022-37966	Elevation of Privilege	Critical	No	No	1
			CVE-2022-41086	Elevation of Privilege	Important	No	No	2
			CVE-2022-41125	Elevation of Privilege	Important	No	Yes	0
			CVE-2022-41088	Remote Code Execution	Critical	No	No	2
			CVE-2022-41058	Denial of Service	Important	No	No	1
			CVE-2022-41039	Remote Code Execution	Critical	No	No	2
			CVE-2022-41109	Elevation of Privilege	Important	No	No	1
			CVE-2022-41056	Denial of Service	Important	No	No	2
			CVE-2022-41098	Information Disclosure	Important	No	No	2

			CVE-2022-41057	Elevation of Privilege	Important	No	No	1
5020019	高危	November 8, 2022 — KB5020019 (Monthly Rollup) for Windows Server 2008 Datacenter ESU,Windows Server 2008 Standard ESU,Windows Server 2008 Enterprise ESU	CVE-2022-23824	Information Disclosure	Important	No	No	2
			CVE-2022-41057	Elevation of Privilege	Important	No	No	1
			CVE-2022-41053	Denial of Service	Important	No	No	2
			CVE-2022-37992	Elevation of Privilege	Important	No	No	2
			CVE-2022-41097	Information Disclosure	Important	No	No	2
			CVE-2022-41073	Elevation of Privilege	Important	No	Yes	0
			CVE-2022-41048	Remote Code Execution	Important	No	No	2
			CVE-2022-38023	Elevation of Privilege	Important	No	No	1
			CVE-2022-41045	Elevation of Privilege	Important	No	No	2
			CVE-2022-41095	Elevation of Privilege	Important	No	No	2
			CVE-2022-41047	Remote Code Execution	Important	No	No	2
			CVE-2022-37966	Elevation of Privilege	Critical	No	No	1
			CVE-2022-41086	Elevation of Privilege	Important	No	No	2

			CVE-2022-41058	Denial of Service	Important	No	No	1
			CVE-2022-41109	Elevation of Privilege	Important	No	No	1
			CVE-2022-41056	Denial of Service	Important	No	No	2
			CVE-2022-41098	Information Disclosure	Important	No	No	2
			CVE-2022-41044	Remote Code Execution	Critical	No	No	2
			CVE-2022-37967	Elevation of Privilege	Critical	No	No	1
5020614	高危	November 8, 2022-KB5020614 Cumulative Update for .NET Framework 4.8 for Windows 10, version 1607 and Windows	CVE-2022-41064	Information Disclosure	Important	No	No	2

		Server 2016						
5020622	高危	November 8, 2022-KB5020622 Cumulative Update for .NET Framework 3.5 and 4.8.1 for Windows 11, version 22H2	CVE-2022-41064	Information Disclosure	Important	No	No	2
5020688	高危	November 8, 2022-Security and Quality Rollup for .NET Framework 3.5.1,	CVE-2022-41064	Information Disclosure	Important	No	No	2

		4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Windows 7 SP1 and Windows Server 2008 R2 SP1 (KB5020688)						
5020686	高危	November 8, 2022-KB5020686 Cumulative Update for .NET Framework 3.5, 4.8 and 4.8.1 for Windows	CVE-2022-41064	Information Disclosure	Important	No	No	2

		10, version 20H2						
5020685	高危	November 8, 2022-KB5020685 Cumulative Update for .NET Framework 3.5, 4.7.2 and 4.8 for Windows 10, version 1809 and Windows Server 2019	CVE-2022-41064	Information Disclosure	Important	No	No	2
5020690	高危	November 8, 2022-Security and Quality	CVE-2022-41064	Information Disclosure	Important	No	No	2

		Rollup for .NET Framework 3.5, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Windows 8.1, RT 8.1, and Windows Server 2012 R2 (KB5020690)						
5019961	高危	November 8, 2022 — KB5019961 (OS Build 22000.1219) for Windows 11 version	CVE-2022-38015	Denial of Service	Critical	No	No	2
			CVE-2022-23824	Information Disclosure	Important	No	No	2
			CVE-2022-41053	Denial of Service	Important	No	No	2
			CVE-2022-41101	Elevation of Privilege	Important	No	No	2
			CVE-2022-41093	Elevation of Privilege	Important	No	No	2
			CVE-2022-41113	Elevation of	Important	No	No	1

		21H2, all editions		Privilege				
			CVE-2022-41055	Information Disclosure	Important	No	No	1
			CVE-2022-41092	Elevation of Privilege	Important	No	No	1
			CVE-2022-41128	Remote Code Execution	Critical	No	Yes	0
			CVE-2022-41049	Security Feature Bypass	Important	No	No	1
			CVE-2022-37992	Elevation of Privilege	Important	No	No	2
			CVE-2022-41091	Security Feature Bypass	Important	Yes	Yes	0
			CVE-2022-41097	Information Disclosure	Important	No	No	2
			CVE-2022-41099	Security Feature Bypass	Important	No	No	2
			CVE-2022-41100	Elevation of Privilege	Important	No	No	2
			CVE-2022-41090	Denial of Service	Important	No	No	1
			CVE-2022-41073	Elevation of Privilege	Important	No	Yes	0
			CVE-2022-41048	Remote Code Execution	Important	No	No	2

			CVE-2022-41052	Remote Code Execution	Important	No	No	2
			CVE-2022-41102	Elevation of Privilege	Important	No	No	2
			CVE-2022-41118	Remote Code Execution	Critical	No	No	1
			CVE-2022-41045	Elevation of Privilege	Important	No	No	2
			CVE-2022-41095	Elevation of Privilege	Important	No	No	2
			CVE-2022-41114	Elevation of Privilege	Important	No	No	2
			CVE-2022-41047	Remote Code Execution	Important	No	No	2
			CVE-2022-41096	Elevation of Privilege	Important	No	No	1
			CVE-2022-41086	Elevation of Privilege	Important	No	No	2
			CVE-2022-41125	Elevation of Privilege	Important	No	Yes	0
			CVE-2022-41050	Elevation of Privilege	Important	No	No	2
			CVE-2022-41088	Remote Code Execution	Critical	No	No	2
			CVE-2022-41058	Denial of Service	Important	No	No	1
			CVE-2022-41039	Remote Code Execution	Critical	No	No	2

			CVE-2022-41109	Elevation of Privilege	Important	No	No	1
			CVE-2022-41056	Denial of Service	Important	No	No	2
			CVE-2022-41098	Information Disclosure	Important	No	No	2
			CVE-2022-41054	Elevation of Privilege	Important	No	No	2
			CVE-2022-41057	Elevation of Privilege	Important	No	No	1
5020023	高危	November 8, 2022 — KB5020023 (Monthly Rollup) for Windows 8.1,Windows RT 8.1,Windows Server 2012 R2,Windows Embedded	CVE-2022-23824	Information Disclosure	Important	No	No	2
			CVE-2022-41053	Denial of Service	Important	No	No	2
			CVE-2022-41093	Elevation of Privilege	Important	No	No	2
			CVE-2022-41128	Remote Code Execution	Critical	No	Yes	0
			CVE-2022-37992	Elevation of Privilege	Important	No	No	2
			CVE-2022-41097	Information Disclosure	Important	No	No	2
			CVE-2022-37967	Elevation of Privilege	Critical	No	No	1
			CVE-2022-41100	Elevation of Privilege	Important	No	No	2
			CVE-2022-41090	Denial of Service	Important	No	No	1

		8.1 Industry Enterprise,Windows Embedded 8.1 Industry Pro	CVE-2022-41073	Elevation of Privilege	Important	No	Yes	0
			CVE-2022-41048	Remote Code Execution	Important	No	No	2
			CVE-2022-38023	Elevation of Privilege	Important	No	No	1
			CVE-2022-41118	Remote Code Execution	Critical	No	No	1
			CVE-2022-41045	Elevation of Privilege	Important	No	No	2
			CVE-2022-41095	Elevation of Privilege	Important	No	No	2
			CVE-2022-41047	Remote Code Execution	Important	No	No	2
			CVE-2022-37966	Elevation of Privilege	Critical	No	No	1
			CVE-2022-41086	Elevation of Privilege	Important	No	No	2
			CVE-2022-41125	Elevation of Privilege	Important	No	Yes	0
			CVE-2022-41088	Remote Code Execution	Critical	No	No	2
			CVE-2022-41058	Denial of Service	Important	No	No	1
			CVE-2022-41039	Remote Code Execution	Critical	No	No	2
			CVE-2022-41109	Elevation of Privilege	Important	No	No	1

			CVE-2022-41056	Denial of Service	Important	No	No	2
			CVE-2022-41098	Information Disclosure	Important	No	No	2
			CVE-2022-41057	Elevation of Privilege	Important	No	No	1
5019980	高危	November 8, 2022 — KB5019980 (OS Build 22621.819) for Windows 11 version 22H2, all editions	CVE-2022-38015	Denial of Service	Critical	No	No	2
			CVE-2022-23824	Information Disclosure	Important	No	No	2
			CVE-2022-41053	Denial of Service	Important	No	No	2
			CVE-2022-41101	Elevation of Privilege	Important	No	No	2
			CVE-2022-41093	Elevation of Privilege	Important	No	No	2
			CVE-2022-41113	Elevation of Privilege	Important	No	No	1
			CVE-2022-41055	Information Disclosure	Important	No	No	1
			CVE-2022-41092	Elevation of Privilege	Important	No	No	1
			CVE-2022-41128	Remote Code Execution	Critical	No	Yes	0
			CVE-2022-41049	Security Feature Bypass	Important	No	No	1
			CVE-2022-37992	Elevation of	Important	No	No	2

				Privilege				
			CVE-2022-41091	Security Feature Bypass	Important	Yes	Yes	0
			CVE-2022-41097	Information Disclosure	Important	No	No	2
			CVE-2022-41099	Security Feature Bypass	Important	No	No	2
			CVE-2022-41100	Elevation of Privilege	Important	No	No	2
			CVE-2022-41090	Denial of Service	Important	No	No	1
			CVE-2022-41073	Elevation of Privilege	Important	No	Yes	0
			CVE-2022-41048	Remote Code Execution	Important	No	No	2
			CVE-2022-41102	Elevation of Privilege	Important	No	No	2
			CVE-2022-41118	Remote Code Execution	Critical	No	No	1
			CVE-2022-41045	Elevation of Privilege	Important	No	No	2
			CVE-2022-41095	Elevation of Privilege	Important	No	No	2
			CVE-2022-41114	Elevation of Privilege	Important	No	No	2
			CVE-2022-41047	Remote Code	Important	No	No	2

				Execution				
			CVE-2022-41096	Elevation of Privilege	Important	No	No	1
			CVE-2022-41086	Elevation of Privilege	Important	No	No	2
			CVE-2022-41125	Elevation of Privilege	Important	No	Yes	0
			CVE-2022-41050	Elevation of Privilege	Important	No	No	2
			CVE-2022-41088	Remote Code Execution	Critical	No	No	2
			CVE-2022-41058	Denial of Service	Important	No	No	1
			CVE-2022-41039	Remote Code Execution	Critical	No	No	2
			CVE-2022-41109	Elevation of Privilege	Important	No	No	1
			CVE-2022-41056	Denial of Service	Important	No	No	2
			CVE-2022-41098	Information Disclosure	Important	No	No	2
			CVE-2022-41054	Elevation of Privilege	Important	No	No	2
			CVE-2022-41057	Elevation of Privilege	Important	No	No	1
5020680	高危	November 8, 2022-Security	CVE-2022-41064	Information Disclosure	Important	No	No	2

		Only Update for .NET Framework 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Windows Server 2012 R2 (KB5020680)						
5020013	高危	November 8, 2022 — KB5020013 (Security-only update) for Windows 7 Enterprise ESU,Wind	CVE-2022-41116	Denial of Service	Important	No	No	2
			CVE-2022-23824	Information Disclosure	Important	No	No	2
			CVE-2022-41057	Elevation of Privilege	Important	No	No	1
			CVE-2022-41053	Denial of Service	Important	No	No	2
			CVE-2022-41128	Remote Code Execution	Critical	No	Yes	0
			CVE-2022-37992	Elevation of Privilege	Important	No	No	2
			CVE-2022-41097	Information Disclosure	Important	No	No	2

		ows 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	CVE-2022-41090	Denial of Service	Important	No	No	1
			CVE-2022-41073	Elevation of Privilege	Important	No	Yes	0
			CVE-2022-41048	Remote Code Execution	Important	No	No	2
			CVE-2022-38023	Elevation of Privilege	Important	No	No	1
			CVE-2022-41118	Remote Code Execution	Critical	No	No	1
			CVE-2022-41045	Elevation of Privilege	Important	No	No	2
			CVE-2022-41095	Elevation of Privilege	Important	No	No	2
			CVE-2022-41047	Remote Code Execution	Important	No	No	2
			CVE-2022-37966	Elevation of Privilege	Critical	No	No	1
			CVE-2022-41086	Elevation of Privilege	Important	No	No	2
			CVE-2022-41058	Denial of Service	Important	No	No	1
			CVE-2022-41039	Remote Code Execution	Critical	No	No	2
			CVE-2022-41109	Elevation of Privilege	Important	No	No	1
			CVE-2022-41056	Denial of Service	Important	No	No	2

		ESU,Windows Embedded POSReady 7 ESU	CVE-2022-41098	Information Disclosure	Important	No	No	2
			CVE-2022-41044	Remote Code Execution	Critical	No	No	2
			CVE-2022-37967	Elevation of Privilege	Critical	No	No	1
5020678	高危	November 8, 2022—Security Only Update for .NET Framework 3.5.1, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Windows 7 SP1 and Windows Server 2008 R2 SP1 (KB5020678)	CVE-2022-41064	Information Disclosure	Important	No	No	2

5019959	高危	November 8, 2022 — KB5019959 (OS Builds 19042.2251, 19043.2251, 19044.2251, and 19045.2251) for Windows 10 Enterprise Multi-Session, version 20H2, Windows 10 Enterprise and Education, version	CVE-2022-38015	Denial of Service	Critical	No	No	2
			CVE-2022-23824	Information Disclosure	Important	No	No	2
			CVE-2022-41053	Denial of Service	Important	No	No	2
			CVE-2022-41101	Elevation of Privilege	Important	No	No	2
			CVE-2022-41093	Elevation of Privilege	Important	No	No	2
			CVE-2022-41113	Elevation of Privilege	Important	No	No	1
			CVE-2022-41055	Information Disclosure	Important	No	No	1
			CVE-2022-41092	Elevation of Privilege	Important	No	No	1
			CVE-2022-41128	Remote Code Execution	Critical	No	Yes	0
			CVE-2022-41049	Security Feature Bypass	Important	No	No	1
			CVE-2022-37992	Elevation of Privilege	Important	No	No	2
			CVE-2022-41091	Security Feature Bypass	Important	Yes	Yes	0
			CVE-2022-41097	Information Disclosure	Important	No	No	2

		20H2,Windows 10 IoT Enterprise, version 20H2,Windows 10 on Surface Hub,Windows 10, version 21H1, all editions,Windows 10, version 21H2, all editions,Windows 10, version 22H2, all editions	CVE-2022-41099	Security Feature Bypass	Important	No	No	2
			CVE-2022-41100	Elevation of Privilege	Important	No	No	2
			CVE-2022-41090	Denial of Service	Important	No	No	1
			CVE-2022-41073	Elevation of Privilege	Important	No	Yes	0
			CVE-2022-41048	Remote Code Execution	Important	No	No	2
			CVE-2022-41052	Remote Code Execution	Important	No	No	2
			CVE-2022-41102	Elevation of Privilege	Important	No	No	2
			CVE-2022-41118	Remote Code Execution	Critical	No	No	1
			CVE-2022-41045	Elevation of Privilege	Important	No	No	2
			CVE-2022-41095	Elevation of Privilege	Important	No	No	2
			CVE-2022-41114	Elevation of Privilege	Important	No	No	2
			CVE-2022-41047	Remote Code Execution	Important	No	No	2
			CVE-2022-41096	Elevation of Privilege	Important	No	No	1
			CVE-2022-41086	Elevation of	Important	No	No	2

				Privilege				
			CVE-2022-41125	Elevation of Privilege	Important	No	Yes	0
			CVE-2022-41050	Elevation of Privilege	Important	No	No	2
			CVE-2022-41088	Remote Code Execution	Critical	No	No	2
			CVE-2022-41058	Denial of Service	Important	No	No	1
			CVE-2022-41039	Remote Code Execution	Critical	No	No	2
			CVE-2022-41109	Elevation of Privilege	Important	No	No	1
			CVE-2022-41056	Denial of Service	Important	No	No	2
			CVE-2022-41098	Information Disclosure	Important	No	No	2
			CVE-2022-41054	Elevation of Privilege	Important	No	No	2
			CVE-2022-41057	Elevation of Privilege	Important	No	No	1
5020687	高危	November 8, 2022-KB5020687 Cumulative Update	CVE-2022-41064	Information Disclosure	Important	No	No	2

		for .NET Framework 3.5, 4.8 and 4.8.1 for Windows 10 Version 21H2						
5020801	高危	November 8, 2022-KB5020801 Cumulative Update for .NET Framework 3.5, 4.8 and 4.8.1 for Windows 10 Version 21H1	CVE-2022-41064	Information Disclosure	Important	No	No	2
5020695	高危	November	CVE-2022-41064	Information	Important	No	No	2

		8, 2022-KB5020695 Cumulative Update for .NET Framework 3.5, 4.8 and 4.8.1 for Windows 11		Disclosure				
5020009	高危	November 8, 2022 — KB5020009 (Monthly Rollup) for Windows Server 2012,Windows Embedded 8	CVE-2022-23824	Information Disclosure	Important	No	No	2
			CVE-2022-41057	Elevation of Privilege	Important	No	No	1
			CVE-2022-41053	Denial of Service	Important	No	No	2
			CVE-2022-41128	Remote Code Execution	Critical	No	Yes	0
			CVE-2022-37992	Elevation of Privilege	Important	No	No	2
			CVE-2022-41097	Information Disclosure	Important	No	No	2
			CVE-2022-41090	Denial of Service	Important	No	No	1

		Standard	CVE-2022-41073	Elevation of Privilege	Important	No	Yes	0
			CVE-2022-41048	Remote Code Execution	Important	No	No	2
			CVE-2022-38023	Elevation of Privilege	Important	No	No	1
			CVE-2022-41045	Elevation of Privilege	Important	No	No	2
			CVE-2022-41095	Elevation of Privilege	Important	No	No	2
			CVE-2022-41047	Remote Code Execution	Important	No	No	2
			CVE-2022-37966	Elevation of Privilege	Critical	No	No	1
			CVE-2022-41086	Elevation of Privilege	Important	No	No	2
			CVE-2022-41125	Elevation of Privilege	Important	No	Yes	0
			CVE-2022-41088	Remote Code Execution	Critical	No	No	2
			CVE-2022-41058	Denial of Service	Important	No	No	1
			CVE-2022-41039	Remote Code Execution	Critical	No	No	2
			CVE-2022-41109	Elevation of Privilege	Important	No	No	1
			CVE-2022-41056	Denial of Service	Important	No	No	2

			CVE-2022-41098	Information Disclosure	Important	No	No	2
			CVE-2022-37967	Elevation of Privilege	Critical	No	No	1
5019964	高危	November 8, 2022 — KB5019964 (OS Build 14393.5501) for Windows 10, version 1607, all editions ,Windows Server 2016, all editions	CVE-2022-38015	Denial of Service	Critical	No	No	2
			CVE-2022-23824	Information Disclosure	Important	No	No	2
			CVE-2022-41053	Denial of Service	Important	No	No	2
			CVE-2022-41101	Elevation of Privilege	Important	No	No	2
			CVE-2022-41093	Elevation of Privilege	Important	No	No	2
			CVE-2022-41128	Remote Code Execution	Critical	No	Yes	0
			CVE-2022-41049	Security Feature Bypass	Important	No	No	1
			CVE-2022-37992	Elevation of Privilege	Important	No	No	2
			CVE-2022-41091	Security Feature Bypass	Important	Yes	Yes	0
			CVE-2022-41097	Information Disclosure	Important	No	No	2
			CVE-2022-41099	Security Feature	Important	No	No	2

				Bypass				
			CVE-2022-37967	Elevation of Privilege	Critical	No	No	1
			CVE-2022-41100	Elevation of Privilege	Important	No	No	2
			CVE-2022-41090	Denial of Service	Important	No	No	1
			CVE-2022-41073	Elevation of Privilege	Important	No	Yes	0
			CVE-2022-41048	Remote Code Execution	Important	No	No	2
			CVE-2022-41052	Remote Code Execution	Important	No	No	2
			CVE-2022-38023	Elevation of Privilege	Important	No	No	1
			CVE-2022-41102	Elevation of Privilege	Important	No	No	2
			CVE-2022-41118	Remote Code Execution	Critical	No	No	1
			CVE-2022-41045	Elevation of Privilege	Important	No	No	2
			CVE-2022-41095	Elevation of Privilege	Important	No	No	2
			CVE-2022-41047	Remote Code Execution	Important	No	No	2
			CVE-2022-37966	Elevation of Privilege	Critical	No	No	1
			CVE-2022-41086	Elevation of	Important	No	No	2

				Privilege				
			CVE-2022-41125	Elevation of Privilege	Important	No	Yes	0
			CVE-2022-41050	Elevation of Privilege	Important	No	No	2
			CVE-2022-41088	Remote Code Execution	Critical	No	No	2
			CVE-2022-41058	Denial of Service	Important	No	No	1
			CVE-2022-41039	Remote Code Execution	Critical	No	No	2
			CVE-2022-41109	Elevation of Privilege	Important	No	No	1
			CVE-2022-41056	Denial of Service	Important	No	No	2
			CVE-2022-41098	Information Disclosure	Important	No	No	2
			CVE-2022-41054	Elevation of Privilege	Important	No	No	2
			CVE-2022-41057	Elevation of Privilege	Important	No	No	1
5019970	高危	November 8, 2022 — KB5019970 (OS Build 10240.19	CVE-2022-38015	Denial of Service	Critical	No	No	2
			CVE-2022-23824	Information Disclosure	Important	No	No	2
			CVE-2022-41064	Information Disclosure	Important	No	No	2
			CVE-2022-41053	Denial of	Important	No	No	2

		567) for Windows 10		Service				
			CVE-2022-41101	Elevation of Privilege	Important	No	No	2
			CVE-2022-41093	Elevation of Privilege	Important	No	No	2
			CVE-2022-41128	Remote Code Execution	Critical	No	Yes	0
			CVE-2022-41049	Security Feature Bypass	Important	No	No	1
			CVE-2022-37992	Elevation of Privilege	Important	No	No	2
			CVE-2022-41091	Security Feature Bypass	Important	Yes	Yes	0
			CVE-2022-41097	Information Disclosure	Important	No	No	2
			CVE-2022-41099	Security Feature Bypass	Important	No	No	2
			CVE-2022-41100	Elevation of Privilege	Important	No	No	2
			CVE-2022-41090	Denial of Service	Important	No	No	1
			CVE-2022-41073	Elevation of Privilege	Important	No	Yes	0
			CVE-2022-41048	Remote Code Execution	Important	No	No	2

			CVE-2022-41052	Remote Code Execution	Important	No	No	2
			CVE-2022-41102	Elevation of Privilege	Important	No	No	2
			CVE-2022-41118	Remote Code Execution	Critical	No	No	1
			CVE-2022-41045	Elevation of Privilege	Important	No	No	2
			CVE-2022-41095	Elevation of Privilege	Important	No	No	2
			CVE-2022-41047	Remote Code Execution	Important	No	No	2
			CVE-2022-41086	Elevation of Privilege	Important	No	No	2
			CVE-2022-41125	Elevation of Privilege	Important	No	Yes	0
			CVE-2022-41050	Elevation of Privilege	Important	No	No	2
			CVE-2022-41088	Remote Code Execution	Critical	No	No	2
			CVE-2022-41058	Denial of Service	Important	No	No	1
			CVE-2022-41039	Remote Code Execution	Critical	No	No	2
			CVE-2022-41109	Elevation of Privilege	Important	No	No	1
			CVE-2022-41056	Denial of Service	Important	No	No	2

			CVE-2022-41098	Information Disclosure	Important	No	No	2
			CVE-2022-41057	Elevation of Privilege	Important	No	No	1
5020689	高危	November 8, 2022-Security and Quality Rollup for .NET Framework 3.5, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Windows Server 2012 (KB5020689)	CVE-2022-41064	Information Disclosure	Important	No	No	2
5020681	高危	November 8, 2022-Security Only Update	CVE-2022-41064	Information Disclosure	Important	No	No	2

		for .NET Framework 4.6.2 for Windows Server 2008 SP2 (KB5020681)						
5019966	高危	November 8, 2022 — KB5019966 (OS Build 17763.3650) for Windows 10 Enterprise 2019 LTSC, Windows 10 IoT Enterprise 2019 LTSC, Windows 10	CVE-2022-38015	Denial of Service	Critical	No	No	2
			CVE-2022-23824	Information Disclosure	Important	No	No	2
			CVE-2022-41053	Denial of Service	Important	No	No	2
			CVE-2022-41101	Elevation of Privilege	Important	No	No	2
			CVE-2022-41093	Elevation of Privilege	Important	No	No	2
			CVE-2022-41113	Elevation of Privilege	Important	No	No	1
			CVE-2022-41055	Information Disclosure	Important	No	No	1
			CVE-2022-41128	Remote Code Execution	Critical	No	Yes	0
			CVE-2022-41049	Security Feature Bypass	Important	No	No	1

		IoT Core 2019 LTSC,Windows Server 2019	CVE-2022-37992	Elevation of Privilege	Important	No	No	2
			CVE-2022-41091	Security Feature Bypass	Important	Yes	Yes	0
			CVE-2022-41097	Information Disclosure	Important	No	No	2
			CVE-2022-41099	Security Feature Bypass	Important	No	No	2
			CVE-2022-37967	Elevation of Privilege	Critical	No	No	1
			CVE-2022-41100	Elevation of Privilege	Important	No	No	2
			CVE-2022-41090	Denial of Service	Important	No	No	1
			CVE-2022-41073	Elevation of Privilege	Important	No	Yes	0
			CVE-2022-41048	Remote Code Execution	Important	No	No	2
			CVE-2022-41052	Remote Code Execution	Important	No	No	2
			CVE-2022-38023	Elevation of Privilege	Important	No	No	1
			CVE-2022-41102	Elevation of Privilege	Important	No	No	2
			CVE-2022-41118	Remote Code Execution	Critical	No	No	1

			CVE-2022-41045	Elevation of Privilege	Important	No	No	2
			CVE-2022-41095	Elevation of Privilege	Important	No	No	2
			CVE-2022-41047	Remote Code Execution	Important	No	No	2
			CVE-2022-37966	Elevation of Privilege	Critical	No	No	1
			CVE-2022-41096	Elevation of Privilege	Important	No	No	1
			CVE-2022-41086	Elevation of Privilege	Important	No	No	2
			CVE-2022-41125	Elevation of Privilege	Important	No	Yes	0
			CVE-2022-41050	Elevation of Privilege	Important	No	No	2
			CVE-2022-41088	Remote Code Execution	Critical	No	No	2
			CVE-2022-41058	Denial of Service	Important	No	No	1
			CVE-2022-41039	Remote Code Execution	Critical	No	No	2
			CVE-2022-41109	Elevation of Privilege	Important	No	No	1
5020691	高危	November 8, 2022-Security and	CVE-2022-41064	Information Disclosure	Important	No	No	2

		Quality Rollup for .NET Framework 2.0, 3.0, 4.6.2 for Windows Server 2008 SP2 (KB5020691)						

本月微软发布的软件安全更新补丁共 12 个，详细列表如下：

KBID	奇安信集团级别	软件名称	CVE 编号	漏洞的影响	漏洞等级	公开披露	已受攻击	漏洞的可利用性
5002305	高危	Description of the security update for SharePoint Enterprise Server 2016:	CVE-2022-41103	Information Disclosure	Important	No	No	2
			CVE-2022-41061	Remote Code Execution	Important	No	No	2

		November 8, 2022 (KB5002305)	CVE-2022-41060	Information Disclosure	Important	No	No	2
			CVE-2022-41062	Remote Code Execution	Important	No	No	2
5002253	高危	Description of the security update for Excel 2016: November 8, 2022 (KB5002253)	CVE-2022-41106	Remote Code Execution	Important	No	No	2
			CVE-2022-41063	Remote Code Execution	Important	No	No	2
			CVE-2022-41104	Security Feature Bypass	Important	No	No	2
3191869	高危	Description of the security update for Office 2016: November 8, 2022 (KB3191869	ADV220003	Defense in Depth	Important	No	No	2

		)						
5019758	高危	Description of the security update for Microsoft Exchange Server 2019, 2016, and 2013: November 8, 2022 (KB5019758)	CVE-2022-41078	Spoofing	Important	No	No	2
			CVE-2022-41123	Elevation of Privilege	Important	No	No	1
			CVE-2022-41080	Elevation of Privilege	Critical	No	No	1
			CVE-2022-41079	Spoofing	Important	No	No	1
5002275	高危	Description of the security update for Excel 2013: November 8, 2022 (KB5002275)	CVE-2022-41106	Remote Code Execution	Important	No	No	2
			CVE-2022-41063	Remote Code Execution	Important	No	No	2
			CVE-2022-41104	Security Feature Bypass	Important	No	No	2
5002223	高危	Description of the security	CVE-2022-41103	Information Disclosu	Important	No	No	2

		update for Word 2016: November 8, 2022 (KB5002223)		re				
			CVE-2022-41061	Remote Code Execution	Important	No	No	2
			CVE-2022-41060	Information Disclosure	Important	No	No	2
5002303	高危	Description of the security update for SharePoint Foundation 2013: November 8, 2022 (KB5002303)	CVE-2022-41062	Remote Code Execution	Important	No	No	2
3191875	高危	Description of the security update for Office 2013: November 8, 2022	ADV220003	Defense in Depth	Important	No	No	2

		(KB3191875)						
5002217	高危	Description of the security update for Word 2013: November 8, 2022 (KB5002217)	CVE-2022-41103	Information Disclosure	Important	No	No	2
			CVE-2022-41061	Remote Code Execution	Important	No	No	2
			CVE-2022-41060	Information Disclosure	Important	No	No	2
5002235	高危	Description of the security update for SharePoint Enterprise Server 2013: November 8, 2022 (KB5002235)	CVE-2022-41103	Information Disclosure	Important	No	No	2
			CVE-2022-41061	Remote Code Execution	Important	No	No	2
			CVE-2022-41060	Information Disclosure	Important	No	No	2
5019958	高危	KB5019958: Cumulative	CVE-2022-41128	Remote Code	Critical	No	Yes	0

		security update for Internet Explorer: November 8, 2022		Execution				
			CVE-2022-41118	Remote Code Execution	Critical	No	No	1
5002261	高危	Description of the security update for Office Web Apps Server 2013: November 8, 2022 (KB5002261)	CVE-2022-41103	Information Disclosure	Important	No	No	2
			CVE-2022-41060	Information Disclosure	Important	No	No	2
			CVE-2022-41061	Remote Code Execution	Important	No	No	2
			CVE-2022-41106	Remote Code Execution	Important	No	No	2
			CVE-2022-41063	Remote Code Execution	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
5002306	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