奇安信集团 2022 年 9 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 9 月 16 日

目 录

文档信息

文档名称	奇安信集团 2022 年 9 月补丁库更新通告		
文档编号	Qi An Xin Group-MSPatch-2022-0916		
发布日期	2022-09-16	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:2022.09.14.1,V10 版本:2022.09.15.1000)已发布，本次更新推送了 25 个微软安全补丁，修复了 54 个安全漏洞，其中 3 个微软官方评级为“严重(Critical)”，51 个评级为“重要(Important)”，这些漏洞影响产品 Windows 和 Microsoft Office。同时推送了 3 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 8 个安全漏洞经奇安信评估满足以下任一条件，需要重点关注。

1. 漏洞等级（Severity）=严重（Critical），
2. 公开披露（Publicly Disclosed）=是（Yes），
3. 已受攻击（Exploited）=是（Yes），
4. 漏洞的可利用性（Exploitability Assessment）="已被利用（Exploitation Detected）" 或 "很可能被利用（Exploitation More Likely）"

详情如下：

KBID	修复的漏洞	漏洞的影响	漏洞等级	公开披露	已受攻击	漏洞的可利用性
5017315 5017328 5017305 5017367 5017377 5017365 5017308 5017370 5017327	CVE-2022-34725	Elevation of Privilege	Important	No	No	Exploitation More Likely
5017315 5017328 5017305 5017308	CVE-2022-37957	Elevation of Privilege	Important	No	No	Exploitation More Likely
5017315 5017328 5017305 5017367 5017377 5017365 5017308 5017358 5017370 5017371 5017327 5017361 5017373	CVE-2022-34718	Remote Code Execution	Critical	No	No	Exploitation More Likely

5017315 5017328 5017305 5017367 5017377 5017365 5017308 5017358 5017370 5017371 5017327 5017361 5017373	CVE-2022-37969	Elevation of Privilege	Important	Yes	Yes	Exploitation Detected
5017315 5017328 5017305 5017367 5017377 5017365 5017308 5017358 5017370 5017371 5017327 5017361 5017373	CVE-2022-35803	Elevation of Privilege	Important	No	No	Exploitation More Likely
5017315 5017328 5017308	CVE-2022-37954	Elevation of Privilege	Important	No	No	Exploitation More Likely
5017315 5017328 5017305 5017367 5017377 5017365 5017308 5017358 5017370 5017371	CVE-2022-34729	Elevation of Privilege	Important	No	No	Exploitation More Likely

5017327 5017361 5017373						
5017328	CVE-2022-23960	Information Disclosure	Important	Yes	No	Exploitation Less Likely

第3章 已知问题和特殊调整

本月暂无已知问题和特殊调整。

第4章 漏洞补丁详细列表

本月微软发布的系统安全更新补丁共 13 个，详细列表如下：

KBID	奇安信集团级别	补丁名称	CVE 编号	漏洞的影响	漏洞等级	公开披露	已受攻击	漏洞的可利用性
5017315	高危	September 13, 2022—KB5017315 (OS Build 17763.3406) for Windows 10 Enterprise 2019 LTSC, Windows 10 IoT Enterprise 2019 LTSC, Windows 10 IoT Core 2019 LTSC, Windows Server 2019	CVE-2022-26929	Remote Code Execution	Important	No	No	2
			CVE-2022-35836	Remote Code Execution	Important	No	No	2
			CVE-2022-34733	Remote Code Execution	Important	No	No	2
			CVE-2022-34721	Remote Code Execution	Critical	No	No	2
			CVE-2022-35833	Denial of Service	Important	No	No	2
			CVE-2022-35830	Remote Code Execution	Important	No	No	2
			CVE-2022-37956	Elevation of Privilege	Important	No	No	2
			CVE-2022-34724	Denial of Service	Important	No	No	2
			CVE-2022-34731	Remote Code Execution	Important	No	No	2
			CVE-2022-33647	Elevation of Privilege	Important	No	No	2
			CVE-2022-35840	Remote Code Execution	Important	No	No	2
			CVE-2022-26928	Elevation of Privilege	Important	No	No	2
			CVE-2022-34728	Information Disclosure	Important	No	No	2
			CVE-2022-30200	Remote Code Execution	Important	No	No	2
			CVE-2022-35	Information	Important	No	No	2

			837	Disclosure				
			CVE-2022-34725	Elevation of Privilege	Important	No	No	1
			CVE-2022-37958	Information Disclosure	Important	No	No	2
			CVE-2022-34722	Remote Code Execution	Critical	No	No	2
			CVE-2022-35841	Remote Code Execution	Important	No	No	2
			CVE-2022-35834	Remote Code Execution	Important	No	No	2
			CVE-2022-34719	Elevation of Privilege	Important	No	No	2
			CVE-2022-38005	Elevation of Privilege	Important	No	No	3
			CVE-2022-34726	Remote Code Execution	Important	No	No	2
			CVE-2022-30196	Denial of Service	Important	No	No	2
			CVE-2022-34730	Remote Code Execution	Important	No	No	2
			CVE-2022-34734	Remote Code Execution	Important	No	No	2
			CVE-2022-35835	Remote Code Execution	Important	No	No	2
			CVE-2022-34727	Remote Code Execution	Important	No	No	2
			CVE-2022-33679	Elevation of Privilege	Important	No	No	2
			CVE-2022-34732	Remote Code Execution	Important	No	No	3
			CVE-2022-38006	Information Disclosure	Important	No	No	2
			CVE-2022-37957	Elevation of Privilege	Important	No	No	1
			CVE-2022-34718	Remote Code Execution	Critical	No	No	1
			CVE-2022-37969	Elevation of Privilege	Important	Yes	Yes	0
			CVE-2022-35831	Information Disclosure	Important	No	No	2

			CVE-2022-34720	Denial of Service	Important	No	No	2
			CVE-2022-35832	Denial of Service	Important	No	No	2
			CVE-2022-35803	Elevation of Privilege	Important	No	No	1
			CVE-2022-37959	Security Feature Bypass	Important	No	No	2
			CVE-2022-37954	Elevation of Privilege	Important	No	No	1
			CVE-2022-30170	Elevation of Privilege	Important	No	No	2
			CVE-2022-37955	Elevation of Privilege	Important	No	No	2
			CVE-2022-34729	Elevation of Privilege	Important	No	No	1
			CVE-2022-38004	Remote Code Execution	Important	No	No	2
5017328	高危	September 13, 2022—KB5017328 (OS Build 22000.978) for Windows 11	CVE-2022-35836	Remote Code Execution	Important	No	No	2
			CVE-2022-34733	Remote Code Execution	Important	No	No	2
			CVE-2022-34721	Remote Code Execution	Critical	No	No	2
			CVE-2022-35833	Denial of Service	Important	No	No	2
			CVE-2022-34723	Information Disclosure	Important	No	No	2
			CVE-2022-37956	Elevation of Privilege	Important	No	No	2
			CVE-2022-38004	Remote Code Execution	Important	No	No	2
			CVE-2022-34731	Remote Code Execution	Important	No	No	2
			CVE-2022-35840	Remote Code Execution	Important	No	No	2
			CVE-2022-26928	Elevation of Privilege	Important	No	No	2
			CVE-2022-34728	Information Disclosure	Important	No	No	2
			CVE-2022-30	Remote Code	Important	No	No	2

			200	Execution				
			CVE-2022-35837	Information Disclosure	Important	No	No	2
			CVE-2022-34722	Remote Code Execution	Critical	No	No	2
			CVE-2022-37958	Information Disclosure	Important	No	No	2
			CVE-2022-35838	Denial of Service	Important	No	No	2
			CVE-2022-35841	Remote Code Execution	Important	No	No	2
			CVE-2022-35834	Remote Code Execution	Important	No	No	2
			CVE-2022-34719	Elevation of Privilege	Important	No	No	2
			CVE-2022-38005	Elevation of Privilege	Important	No	No	3
			CVE-2022-34726	Remote Code Execution	Important	No	No	2
			CVE-2022-30196	Denial of Service	Important	No	No	2
			CVE-2022-34730	Remote Code Execution	Important	No	No	2
			CVE-2022-34734	Remote Code Execution	Important	No	No	2
			CVE-2022-35835	Remote Code Execution	Important	No	No	2
			CVE-2022-34727	Remote Code Execution	Important	No	No	2
			CVE-2022-34732	Remote Code Execution	Important	No	No	3
			CVE-2022-38006	Information Disclosure	Important	No	No	2
			CVE-2022-37957	Elevation of Privilege	Important	No	No	1
			CVE-2022-34718	Remote Code Execution	Critical	No	No	1
			CVE-2022-37969	Elevation of Privilege	Important	Yes	Yes	0
			CVE-2022-35831	Information Disclosure	Important	No	No	2

			CVE-2022-34720	Denial of Service	Important	No	No	2
			CVE-2022-35832	Denial of Service	Important	No	No	2
			CVE-2022-35803	Elevation of Privilege	Important	No	No	1
			CVE-2022-37954	Elevation of Privilege	Important	No	No	1
			CVE-2022-30170	Elevation of Privilege	Important	No	No	2
			CVE-2022-37955	Elevation of Privilege	Important	No	No	2
			CVE-2022-34729	Elevation of Privilege	Important	No	No	1
			CVE-2022-23960	Information Disclosure	Important	Yes	No	2
			CVE-2022-34725	Elevation of Privilege	Important	No	No	1
5017305	高危	September 13, 2022—KB5017305 (OS Build 14393.5356) for Windows 10, version 1607, all editions ,Windows Server 2016, all editions	CVE-2022-26929	Remote Code Execution	Important	No	No	2
			CVE-2022-35836	Remote Code Execution	Important	No	No	2
			CVE-2022-34733	Remote Code Execution	Important	No	No	2
			CVE-2022-34721	Remote Code Execution	Critical	No	No	2
			CVE-2022-35833	Denial of Service	Important	No	No	2
			CVE-2022-35830	Remote Code Execution	Important	No	No	2
			CVE-2022-37956	Elevation of Privilege	Important	No	No	2
			CVE-2022-34724	Denial of Service	Important	No	No	2
			CVE-2022-34731	Remote Code Execution	Important	No	No	2
			CVE-2022-33647	Elevation of Privilege	Important	No	No	2
			CVE-2022-35840	Remote Code Execution	Important	No	No	2
			CVE-2022-26	Elevation of	Important	No	No	2

			928	Privilege				
			CVE-2022-34728	Information Disclosure	Important	No	No	2
			CVE-2022-30200	Remote Code Execution	Important	No	No	2
			CVE-2022-35837	Information Disclosure	Important	No	No	2
			CVE-2022-34725	Elevation of Privilege	Important	No	No	1
			CVE-2022-37958	Information Disclosure	Important	No	No	2
			CVE-2022-34722	Remote Code Execution	Critical	No	No	2
			CVE-2022-35841	Remote Code Execution	Important	No	No	2
			CVE-2022-35834	Remote Code Execution	Important	No	No	2
			CVE-2022-34719	Elevation of Privilege	Important	No	No	2
			CVE-2022-38005	Elevation of Privilege	Important	No	No	3
			CVE-2022-34726	Remote Code Execution	Important	No	No	2
			CVE-2022-34730	Remote Code Execution	Important	No	No	2
			CVE-2022-34734	Remote Code Execution	Important	No	No	2
			CVE-2022-35835	Remote Code Execution	Important	No	No	2
			CVE-2022-34727	Remote Code Execution	Important	No	No	2
			CVE-2022-33679	Elevation of Privilege	Important	No	No	2
			CVE-2022-34732	Remote Code Execution	Important	No	No	3
			CVE-2022-38006	Information Disclosure	Important	No	No	2
			CVE-2022-37957	Elevation of Privilege	Important	No	No	1
			CVE-2022-34718	Remote Code Execution	Critical	No	No	1

			CVE-2022-37969	Elevation of Privilege	Important	Yes	Yes	0
			CVE-2022-35831	Information Disclosure	Important	No	No	2
			CVE-2022-34720	Denial of Service	Important	No	No	2
			CVE-2022-35832	Denial of Service	Important	No	No	2
			CVE-2022-35803	Elevation of Privilege	Important	No	No	1
			CVE-2022-37959	Security Feature Bypass	Important	No	No	2
			CVE-2022-30170	Elevation of Privilege	Important	No	No	2
			CVE-2022-37955	Elevation of Privilege	Important	No	No	2
			CVE-2022-34729	Elevation of Privilege	Important	No	No	1
			CVE-2022-38004	Remote Code Execution	Important	No	No	2
5017367	高危	September 13, 2022—KB5017367 (Monthly Rollup) for Windows 8.1,Windows RT 8.1,Windows Server 2012 R2,Windows Embedded 8.1 Industry Enterpri	CVE-2022-26929	Remote Code Execution	Important	No	No	2
			CVE-2022-35836	Remote Code Execution	Important	No	No	2
			CVE-2022-34733	Remote Code Execution	Important	No	No	2
			CVE-2022-34721	Remote Code Execution	Critical	No	No	2
			CVE-2022-35833	Denial of Service	Important	No	No	2
			CVE-2022-35830	Remote Code Execution	Important	No	No	2
			CVE-2022-37956	Elevation of Privilege	Important	No	No	2
			CVE-2022-34724	Denial of Service	Important	No	No	2
			CVE-2022-38004	Remote Code Execution	Important	No	No	2
			CVE-2022-34731	Remote Code Execution	Important	No	No	2
			CVE-2022-33	Elevation of	Important	No	No	2

		se,Windows Embedded 8.1 Industry Pro	647	Privilege				
			CVE-2022-35840	Remote Code Execution	Important	No	No	2
			CVE-2022-34728	Information Disclosure	Important	No	No	2
			CVE-2022-30200	Remote Code Execution	Important	No	No	2
			CVE-2022-35837	Information Disclosure	Important	No	No	2
			CVE-2022-34722	Remote Code Execution	Critical	No	No	2
			CVE-2022-37958	Information Disclosure	Important	No	No	2
			CVE-2022-35834	Remote Code Execution	Important	No	No	2
			CVE-2022-34719	Elevation of Privilege	Important	No	No	2
			CVE-2022-38005	Elevation of Privilege	Important	No	No	3
			CVE-2022-34726	Remote Code Execution	Important	No	No	2
			CVE-2022-34730	Remote Code Execution	Important	No	No	2
			CVE-2022-34734	Remote Code Execution	Important	No	No	2
			CVE-2022-35835	Remote Code Execution	Important	No	No	2
			CVE-2022-34727	Remote Code Execution	Important	No	No	2
			CVE-2022-33679	Elevation of Privilege	Important	No	No	2
			CVE-2022-34732	Remote Code Execution	Important	No	No	3
			CVE-2022-38006	Information Disclosure	Important	No	No	2
			CVE-2022-34718	Remote Code Execution	Critical	No	No	1
			CVE-2022-37969	Elevation of Privilege	Important	Yes	Yes	0
			CVE-2022-35831	Information Disclosure	Important	No	No	2

			CVE-2022-34720	Denial of Service	Important	No	No	2
			CVE-2022-35832	Denial of Service	Important	No	No	2
			CVE-2022-35803	Elevation of Privilege	Important	No	No	1
			CVE-2022-37959	Security Feature Bypass	Important	No	No	2
			CVE-2022-30170	Elevation of Privilege	Important	No	No	2
			CVE-2022-37955	Elevation of Privilege	Important	No	No	2
			CVE-2022-34729	Elevation of Privilege	Important	No	No	1
			CVE-2022-34725	Elevation of Privilege	Important	No	No	1
5017377	高危	September 13, 2022—KB5017377 (Security-only update) for Windows Server 2012, Windows Embedded 8 Standard	CVE-2022-26929	Remote Code Execution	Important	No	No	2
			CVE-2022-35836	Remote Code Execution	Important	No	No	2
			CVE-2022-34733	Remote Code Execution	Important	No	No	2
			CVE-2022-34721	Remote Code Execution	Critical	No	No	2
			CVE-2022-35833	Denial of Service	Important	No	No	2
			CVE-2022-35830	Remote Code Execution	Important	No	No	2
			CVE-2022-37956	Elevation of Privilege	Important	No	No	2
			CVE-2022-34724	Denial of Service	Important	No	No	2
			CVE-2022-38004	Remote Code Execution	Important	No	No	2
			CVE-2022-34731	Remote Code Execution	Important	No	No	2
			CVE-2022-33647	Elevation of Privilege	Important	No	No	2
			CVE-2022-35840	Remote Code Execution	Important	No	No	2
			CVE-2022-34	Information	Important	No	No	2

			728	Disclosure				
			CVE-2022-30200	Remote Code Execution	Important	No	No	2
			CVE-2022-35837	Information Disclosure	Important	No	No	2
			CVE-2022-34722	Remote Code Execution	Critical	No	No	2
			CVE-2022-37958	Information Disclosure	Important	No	No	2
			CVE-2022-35834	Remote Code Execution	Important	No	No	2
			CVE-2022-34719	Elevation of Privilege	Important	No	No	2
			CVE-2022-38005	Elevation of Privilege	Important	No	No	3
			CVE-2022-34726	Remote Code Execution	Important	No	No	2
			CVE-2022-34730	Remote Code Execution	Important	No	No	2
			CVE-2022-34734	Remote Code Execution	Important	No	No	2
			CVE-2022-35835	Remote Code Execution	Important	No	No	2
			CVE-2022-34727	Remote Code Execution	Important	No	No	2
			CVE-2022-33679	Elevation of Privilege	Important	No	No	2
			CVE-2022-34732	Remote Code Execution	Important	No	No	3
			CVE-2022-38006	Information Disclosure	Important	No	No	2
			CVE-2022-34718	Remote Code Execution	Critical	No	No	1
			CVE-2022-37969	Elevation of Privilege	Important	Yes	Yes	0
			CVE-2022-34720	Denial of Service	Important	No	No	2
			CVE-2022-35803	Elevation of Privilege	Important	No	No	1
			CVE-2022-30170	Elevation of Privilege	Important	No	No	2

			CVE-2022-37955	Elevation of Privilege	Important	No	No	2
			CVE-2022-34729	Elevation of Privilege	Important	No	No	1
			CVE-2022-34725	Elevation of Privilege	Important	No	No	1
5017365	高危	September 13, 2022—KB5017365 (Security-only update) 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-2022-26929	Remote Code Execution	Important	No	No	2
			CVE-2022-35836	Remote Code Execution	Important	No	No	2
			CVE-2022-34733	Remote Code Execution	Important	No	No	2
			CVE-2022-34721	Remote Code Execution	Critical	No	No	2
			CVE-2022-35833	Denial of Service	Important	No	No	2
			CVE-2022-35830	Remote Code Execution	Important	No	No	2
			CVE-2022-37956	Elevation of Privilege	Important	No	No	2
			CVE-2022-34724	Denial of Service	Important	No	No	2
			CVE-2022-38004	Remote Code Execution	Important	No	No	2
			CVE-2022-34731	Remote Code Execution	Important	No	No	2
			CVE-2022-33647	Elevation of Privilege	Important	No	No	2
			CVE-2022-35840	Remote Code Execution	Important	No	No	2
			CVE-2022-34728	Information Disclosure	Important	No	No	2
			CVE-2022-30200	Remote Code Execution	Important	No	No	2
			CVE-2022-35837	Information Disclosure	Important	No	No	2
			CVE-2022-34722	Remote Code Execution	Critical	No	No	2
			CVE-2022-37958	Information Disclosure	Important	No	No	2
			CVE-2022-35	Remote Code	Important	No	No	2

			834	Execution				
			CVE-2022-34719	Elevation of Privilege	Important	No	No	2
			CVE-2022-38005	Elevation of Privilege	Important	No	No	3
			CVE-2022-34726	Remote Code Execution	Important	No	No	2
			CVE-2022-34730	Remote Code Execution	Important	No	No	2
			CVE-2022-34734	Remote Code Execution	Important	No	No	2
			CVE-2022-35835	Remote Code Execution	Important	No	No	2
			CVE-2022-34727	Remote Code Execution	Important	No	No	2
			CVE-2022-33679	Elevation of Privilege	Important	No	No	2
			CVE-2022-34732	Remote Code Execution	Important	No	No	3
			CVE-2022-38006	Information Disclosure	Important	No	No	2
			CVE-2022-34718	Remote Code Execution	Critical	No	No	1
			CVE-2022-37969	Elevation of Privilege	Important	Yes	Yes	0
			CVE-2022-35831	Information Disclosure	Important	No	No	2
			CVE-2022-34720	Denial of Service	Important	No	No	2
			CVE-2022-35832	Denial of Service	Important	No	No	2
			CVE-2022-35803	Elevation of Privilege	Important	No	No	1
			CVE-2022-37959	Security Feature Bypass	Important	No	No	2
			CVE-2022-30170	Elevation of Privilege	Important	No	No	2
			CVE-2022-37955	Elevation of Privilege	Important	No	No	2
			CVE-2022-34729	Elevation of Privilege	Important	No	No	1

			CVE-2022-34725	Elevation of Privilege	Important	No	No	1
5017308	高危	September 13, 2022—KB5017308 (OS Builds 19042.2006, 19043.2006, and 19044.2006) for Windows 10 Enterprise Multi-Session, version 20H2,Windows 10 Enterprise and Education, version 20H2,Windows 10 IoT Enterprise, version 20H2,Windows 10 on Surface Hub,Windows 10, version	CVE-2022-35836	Remote Code Execution	Important	No	No	2
			CVE-2022-34733	Remote Code Execution	Important	No	No	2
			CVE-2022-34721	Remote Code Execution	Critical	No	No	2
			CVE-2022-35833	Denial of Service	Important	No	No	2
			CVE-2022-37956	Elevation of Privilege	Important	No	No	2
			CVE-2022-38004	Remote Code Execution	Important	No	No	2
			CVE-2022-34731	Remote Code Execution	Important	No	No	2
			CVE-2022-35840	Remote Code Execution	Important	No	No	2
			CVE-2022-26928	Elevation of Privilege	Important	No	No	2
			CVE-2022-34728	Information Disclosure	Important	No	No	2
			CVE-2022-30200	Remote Code Execution	Important	No	No	2
			CVE-2022-35837	Information Disclosure	Important	No	No	2
			CVE-2022-34722	Remote Code Execution	Critical	No	No	2
			CVE-2022-37958	Information Disclosure	Important	No	No	2
			CVE-2022-35841	Remote Code Execution	Important	No	No	2
			CVE-2022-35834	Remote Code Execution	Important	No	No	2
			CVE-2022-34719	Elevation of Privilege	Important	No	No	2
			CVE-2022-38005	Elevation of Privilege	Important	No	No	3
			CVE-2022-34726	Remote Code Execution	Important	No	No	2
			CVE-2022-30	Denial of	Important	No	No	2

		21H1, all editions ,Windows 10, version 21H2, all editions	196	Service				
			CVE-2022-34730	Remote Code Execution	Important	No	No	2
			CVE-2022-34734	Remote Code Execution	Important	No	No	2
			CVE-2022-35835	Remote Code Execution	Important	No	No	2
			CVE-2022-34727	Remote Code Execution	Important	No	No	2
			CVE-2022-34732	Remote Code Execution	Important	No	No	3
			CVE-2022-38006	Information Disclosure	Important	No	No	2
			CVE-2022-37957	Elevation of Privilege	Important	No	No	1
			CVE-2022-34718	Remote Code Execution	Critical	No	No	1
			CVE-2022-37969	Elevation of Privilege	Important	Yes	Yes	0
			CVE-2022-35831	Information Disclosure	Important	No	No	2
			CVE-2022-34720	Denial of Service	Important	No	No	2
			CVE-2022-35832	Denial of Service	Important	No	No	2
			CVE-2022-35803	Elevation of Privilege	Important	No	No	1
			CVE-2022-37954	Elevation of Privilege	Important	No	No	1
			CVE-2022-30170	Elevation of Privilege	Important	No	No	2
			CVE-2022-37955	Elevation of Privilege	Important	No	No	2
			CVE-2022-34729	Elevation of Privilege	Important	No	No	1
			CVE-2022-34725	Elevation of Privilege	Important	No	No	1
5017358	高危	September 13, 2022—KB501735	CVE-2022-26929	Remote Code Execution	Important	No	No	2
			CVE-2022-35836	Remote Code Execution	Important	No	No	2

		8 (Monthly Rollup) for Windows Server 2008 Datacenter ESU,Windows Server 2008 Standard ESU,Windows Server 2008 Enterprise ESU	CVE-2022-34733	Remote Code Execution	Important	No	No	2
			CVE-2022-34721	Remote Code Execution	Critical	No	No	2
			CVE-2022-35830	Remote Code Execution	Important	No	No	2
			CVE-2022-37956	Elevation of Privilege	Important	No	No	2
			CVE-2022-34724	Denial of Service	Important	No	No	2
			CVE-2022-34731	Remote Code Execution	Important	No	No	2
			CVE-2022-33647	Elevation of Privilege	Important	No	No	2
			CVE-2022-35840	Remote Code Execution	Important	No	No	2
			CVE-2022-34728	Information Disclosure	Important	No	No	2
			CVE-2022-30200	Remote Code Execution	Important	No	No	2
			CVE-2022-35837	Information Disclosure	Important	No	No	2
			CVE-2022-34722	Remote Code Execution	Critical	No	No	2
			CVE-2022-35834	Remote Code Execution	Important	No	No	2
			CVE-2022-34719	Elevation of Privilege	Important	No	No	2
			CVE-2022-38005	Elevation of Privilege	Important	No	No	3
			CVE-2022-34726	Remote Code Execution	Important	No	No	2
			CVE-2022-34730	Remote Code Execution	Important	No	No	2
			CVE-2022-34734	Remote Code Execution	Important	No	No	2
			CVE-2022-35835	Remote Code Execution	Important	No	No	2
			CVE-2022-34727	Remote Code Execution	Important	No	No	2
			CVE-2022-33	Elevation of	Important	No	No	2

			679	Privilege				
			CVE-2022-34732	Remote Code Execution	Important	No	No	3
			CVE-2022-38006	Information Disclosure	Important	No	No	2
			CVE-2022-34718	Remote Code Execution	Critical	No	No	1
			CVE-2022-37969	Elevation of Privilege	Important	Yes	Yes	0
			CVE-2022-34720	Denial of Service	Important	No	No	2
			CVE-2022-35803	Elevation of Privilege	Important	No	No	1
			CVE-2022-37964	Elevation of Privilege	Important	No	No	2
			CVE-2022-30170	Elevation of Privilege	Important	No	No	2
			CVE-2022-37955	Elevation of Privilege	Important	No	No	2
			CVE-2022-34729	Elevation of Privilege	Important	No	No	1
			CVE-2022-38004	Remote Code Execution	Important	No	No	2
5017370	高危	September 13, 2022—KB5017370 (Monthly Rollup) for Windows Server 2012, Windows Embedded 8 Standard	CVE-2022-26929	Remote Code Execution	Important	No	No	2
			CVE-2022-35836	Remote Code Execution	Important	No	No	2
			CVE-2022-34733	Remote Code Execution	Important	No	No	2
			CVE-2022-34721	Remote Code Execution	Critical	No	No	2
			CVE-2022-35833	Denial of Service	Important	No	No	2
			CVE-2022-35830	Remote Code Execution	Important	No	No	2
			CVE-2022-37956	Elevation of Privilege	Important	No	No	2
			CVE-2022-34724	Denial of Service	Important	No	No	2
			CVE-2022-38004	Remote Code Execution	Important	No	No	2

			CVE-2022-34731	Remote Code Execution	Important	No	No	2
			CVE-2022-33647	Elevation of Privilege	Important	No	No	2
			CVE-2022-35840	Remote Code Execution	Important	No	No	2
			CVE-2022-34728	Information Disclosure	Important	No	No	2
			CVE-2022-30200	Remote Code Execution	Important	No	No	2
			CVE-2022-35837	Information Disclosure	Important	No	No	2
			CVE-2022-34722	Remote Code Execution	Critical	No	No	2
			CVE-2022-37958	Information Disclosure	Important	No	No	2
			CVE-2022-35834	Remote Code Execution	Important	No	No	2
			CVE-2022-34719	Elevation of Privilege	Important	No	No	2
			CVE-2022-38005	Elevation of Privilege	Important	No	No	3
			CVE-2022-34726	Remote Code Execution	Important	No	No	2
			CVE-2022-34730	Remote Code Execution	Important	No	No	2
			CVE-2022-34734	Remote Code Execution	Important	No	No	2
			CVE-2022-35835	Remote Code Execution	Important	No	No	2
			CVE-2022-34727	Remote Code Execution	Important	No	No	2
			CVE-2022-33679	Elevation of Privilege	Important	No	No	2
			CVE-2022-34732	Remote Code Execution	Important	No	No	3
			CVE-2022-38006	Information Disclosure	Important	No	No	2
			CVE-2022-34718	Remote Code Execution	Critical	No	No	1
			CVE-2022-37	Elevation of	Important	Yes	Yes	0

			969	Privilege				
			CVE-2022-34720	Denial of Service	Important	No	No	2
			CVE-2022-35803	Elevation of Privilege	Important	No	No	1
			CVE-2022-30170	Elevation of Privilege	Important	No	No	2
			CVE-2022-37955	Elevation of Privilege	Important	No	No	2
			CVE-2022-34729	Elevation of Privilege	Important	No	No	1
			CVE-2022-34725	Elevation of Privilege	Important	No	No	1
5017371	高危	September 13, 2022—KB5017371 (Security-only update) for Windows Server 2008 Datacenter ESU,Windows Server 2008 Standard ESU,Windows Server 2008 Enterprise ESU	CVE-2022-26929	Remote Code Execution	Important	No	No	2
			CVE-2022-35836	Remote Code Execution	Important	No	No	2
			CVE-2022-34733	Remote Code Execution	Important	No	No	2
			CVE-2022-34721	Remote Code Execution	Critical	No	No	2
			CVE-2022-35830	Remote Code Execution	Important	No	No	2
			CVE-2022-37956	Elevation of Privilege	Important	No	No	2
			CVE-2022-34724	Denial of Service	Important	No	No	2
			CVE-2022-34731	Remote Code Execution	Important	No	No	2
			CVE-2022-33647	Elevation of Privilege	Important	No	No	2
			CVE-2022-35840	Remote Code Execution	Important	No	No	2
			CVE-2022-34728	Information Disclosure	Important	No	No	2
			CVE-2022-30200	Remote Code Execution	Important	No	No	2
			CVE-2022-35837	Information Disclosure	Important	No	No	2
			CVE-2022-34722	Remote Code Execution	Critical	No	No	2

			CVE-2022-35834	Remote Code Execution	Important	No	No	2
			CVE-2022-34719	Elevation of Privilege	Important	No	No	2
			CVE-2022-38005	Elevation of Privilege	Important	No	No	3
			CVE-2022-34726	Remote Code Execution	Important	No	No	2
			CVE-2022-34730	Remote Code Execution	Important	No	No	2
			CVE-2022-34734	Remote Code Execution	Important	No	No	2
			CVE-2022-35835	Remote Code Execution	Important	No	No	2
			CVE-2022-34727	Remote Code Execution	Important	No	No	2
			CVE-2022-33679	Elevation of Privilege	Important	No	No	2
			CVE-2022-34732	Remote Code Execution	Important	No	No	3
			CVE-2022-38006	Information Disclosure	Important	No	No	2
			CVE-2022-34718	Remote Code Execution	Critical	No	No	1
			CVE-2022-37969	Elevation of Privilege	Important	Yes	Yes	0
			CVE-2022-34720	Denial of Service	Important	No	No	2
			CVE-2022-35803	Elevation of Privilege	Important	No	No	1
			CVE-2022-37964	Elevation of Privilege	Important	No	No	2
			CVE-2022-30170	Elevation of Privilege	Important	No	No	2
			CVE-2022-37955	Elevation of Privilege	Important	No	No	2
			CVE-2022-34729	Elevation of Privilege	Important	No	No	1
			CVE-2022-38004	Remote Code Execution	Important	No	No	2
5017327	高危	Septembe	CVE-2022-35	Remote Code	Important	No	No	2

		r 13, 2022—KB5017327 (OS Build 10240.19444) for Windows 10	836	Execution				
			CVE-2022-34733	Remote Code Execution	Important	No	No	2
			CVE-2022-34721	Remote Code Execution	Critical	No	No	2
			CVE-2022-35833	Denial of Service	Important	No	No	2
			CVE-2022-37956	Elevation of Privilege	Important	No	No	2
			CVE-2022-38004	Remote Code Execution	Important	No	No	2
			CVE-2022-34731	Remote Code Execution	Important	No	No	2
			CVE-2022-35840	Remote Code Execution	Important	No	No	2
			CVE-2022-26928	Elevation of Privilege	Important	No	No	2
			CVE-2022-34728	Information Disclosure	Important	No	No	2
			CVE-2022-30200	Remote Code Execution	Important	No	No	2
			CVE-2022-35837	Information Disclosure	Important	No	No	2
			CVE-2022-34722	Remote Code Execution	Critical	No	No	2
			CVE-2022-37958	Information Disclosure	Important	No	No	2
			CVE-2022-35841	Remote Code Execution	Important	No	No	2
			CVE-2022-35834	Remote Code Execution	Important	No	No	2
			CVE-2022-34719	Elevation of Privilege	Important	No	No	2
			CVE-2022-38005	Elevation of Privilege	Important	No	No	3
			CVE-2022-34726	Remote Code Execution	Important	No	No	2
			CVE-2022-34730	Remote Code Execution	Important	No	No	2
			CVE-2022-34734	Remote Code Execution	Important	No	No	2

			CVE-2022-35835	Remote Code Execution	Important	No	No	2
			CVE-2022-34727	Remote Code Execution	Important	No	No	2
			CVE-2022-34732	Remote Code Execution	Important	No	No	3
			CVE-2022-38006	Information Disclosure	Important	No	No	2
			CVE-2022-34718	Remote Code Execution	Critical	No	No	1
			CVE-2022-37969	Elevation of Privilege	Important	Yes	Yes	0
			CVE-2022-35831	Information Disclosure	Important	No	No	2
			CVE-2022-34720	Denial of Service	Important	No	No	2
			CVE-2022-35832	Denial of Service	Important	No	No	2
			CVE-2022-35803	Elevation of Privilege	Important	No	No	1
			CVE-2022-30170	Elevation of Privilege	Important	No	No	2
			CVE-2022-37955	Elevation of Privilege	Important	No	No	2
			CVE-2022-34729	Elevation of Privilege	Important	No	No	1
			CVE-2022-34725	Elevation of Privilege	Important	No	No	1
5017361	高危	September 13, 2022—KB5017361 (Monthly Rollup) for Windows 7 Enterprise ESU,Wind	CVE-2022-26929	Remote Code Execution	Important	No	No	2
			CVE-2022-35836	Remote Code Execution	Important	No	No	2
			CVE-2022-34733	Remote Code Execution	Important	No	No	2
			CVE-2022-34721	Remote Code Execution	Critical	No	No	2
			CVE-2022-35833	Denial of Service	Important	No	No	2
			CVE-2022-35830	Remote Code Execution	Important	No	No	2
			CVE-2022-37	Elevation of	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 ESU,Windows Embedded POSReady 7 ESU	956	Privilege				
			CVE-2022-34724	Denial of Service	Important	No	No	2
			CVE-2022-34731	Remote Code Execution	Important	No	No	2
			CVE-2022-33647	Elevation of Privilege	Important	No	No	2
			CVE-2022-35840	Remote Code Execution	Important	No	No	2
			CVE-2022-34728	Information Disclosure	Important	No	No	2
			CVE-2022-30200	Remote Code Execution	Important	No	No	2
			CVE-2022-35837	Information Disclosure	Important	No	No	2
			CVE-2022-34722	Remote Code Execution	Critical	No	No	2
			CVE-2022-37958	Information Disclosure	Important	No	No	2
			CVE-2022-35834	Remote Code Execution	Important	No	No	2
			CVE-2022-34719	Elevation of Privilege	Important	No	No	2
			CVE-2022-38005	Elevation of Privilege	Important	No	No	3
			CVE-2022-34726	Remote Code Execution	Important	No	No	2
			CVE-2022-34730	Remote Code Execution	Important	No	No	2
			CVE-2022-34734	Remote Code Execution	Important	No	No	2
			CVE-2022-35835	Remote Code Execution	Important	No	No	2
			CVE-2022-34727	Remote Code Execution	Important	No	No	2
			CVE-2022-33679	Elevation of Privilege	Important	No	No	2
			CVE-2022-34732	Remote Code Execution	Important	No	No	3
			CVE-2022-38006	Information Disclosure	Important	No	No	2

			CVE-2022-34718	Remote Code Execution	Critical	No	No	1
			CVE-2022-37969	Elevation of Privilege	Important	Yes	Yes	0
			CVE-2022-34720	Denial of Service	Important	No	No	2
			CVE-2022-35832	Denial of Service	Important	No	No	2
			CVE-2022-35803	Elevation of Privilege	Important	No	No	1
			CVE-2022-37964	Elevation of Privilege	Important	No	No	2
			CVE-2022-30170	Elevation of Privilege	Important	No	No	2
			CVE-2022-37955	Elevation of Privilege	Important	No	No	2
			CVE-2022-34729	Elevation of Privilege	Important	No	No	1
			CVE-2022-38004	Remote Code Execution	Important	No	No	2
5017373	高危	September 13, 2022—KB5017373 (Security-only update) for Windows 7 Enterprise ESU, Windows 7 Professional ESU, Windows 7 Ultimate ESU, Wind	CVE-2022-26929	Remote Code Execution	Important	No	No	2
			CVE-2022-35836	Remote Code Execution	Important	No	No	2
			CVE-2022-34733	Remote Code Execution	Important	No	No	2
			CVE-2022-34721	Remote Code Execution	Critical	No	No	2
			CVE-2022-35833	Denial of Service	Important	No	No	2
			CVE-2022-35830	Remote Code Execution	Important	No	No	2
			CVE-2022-37956	Elevation of Privilege	Important	No	No	2
			CVE-2022-34724	Denial of Service	Important	No	No	2
			CVE-2022-34731	Remote Code Execution	Important	No	No	2
			CVE-2022-33647	Elevation of Privilege	Important	No	No	2
			CVE-2022-35	Remote Code	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	840	Execution				
			CVE-2022-34728	Information Disclosure	Important	No	No	2
			CVE-2022-30200	Remote Code Execution	Important	No	No	2
			CVE-2022-35837	Information Disclosure	Important	No	No	2
			CVE-2022-34722	Remote Code Execution	Critical	No	No	2
			CVE-2022-37958	Information Disclosure	Important	No	No	2
			CVE-2022-35834	Remote Code Execution	Important	No	No	2
			CVE-2022-34719	Elevation of Privilege	Important	No	No	2
			CVE-2022-38005	Elevation of Privilege	Important	No	No	3
			CVE-2022-34726	Remote Code Execution	Important	No	No	2
			CVE-2022-34730	Remote Code Execution	Important	No	No	2
			CVE-2022-34734	Remote Code Execution	Important	No	No	2
			CVE-2022-35835	Remote Code Execution	Important	No	No	2
			CVE-2022-34727	Remote Code Execution	Important	No	No	2
			CVE-2022-33679	Elevation of Privilege	Important	No	No	2
			CVE-2022-34732	Remote Code Execution	Important	No	No	3
			CVE-2022-38006	Information Disclosure	Important	No	No	2
			CVE-2022-34718	Remote Code Execution	Critical	No	No	1
			CVE-2022-37969	Elevation of Privilege	Important	Yes	Yes	0
			CVE-2022-34720	Denial of Service	Important	No	No	2
			CVE-2022-35832	Denial of Service	Important	No	No	2

			CVE-2022-35803	Elevation of Privilege	Important	No	No	1
			CVE-2022-37964	Elevation of Privilege	Important	No	No	2
			CVE-2022-30170	Elevation of Privilege	Important	No	No	2
			CVE-2022-37955	Elevation of Privilege	Important	No	No	2
			CVE-2022-34729	Elevation of Privilege	Important	No	No	1
			CVE-2022-38004	Remote Code Execution	Important	No	No	2

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
5002159	高危	Description of the security update for SharePoint Foundation 2013: September 13, 2022 (KB5002159)	CVE-2022-38008	Remote Code Execution	Important	No	No	2
5002016	高危	Description of the security update for Visio 2016: September 13, 2022 (KB5002016)	CVE-2022-38010	Remote Code Execution	Important	No	No	2
5017497	高危	September 13, 2022-KB5017497 Cumulative Update for .NET Framework 3.5, 4.8 and 4.8.1 for Windows 11	CVE-2022-26929	Remote Code Execution	Important	No	No	2
5002267	高危	Descriptio	CVE-2022-38009	Remote	Important	No	No	2

		n of the security update for SharePoint Foundation 2013: September 13, 2022 (KB5002267)		Code Execution				
			CVE-2022-37961	Remote Code Execution	Important	No	No	3
			CVE-2022-35823	Remote Code Execution	Important	No	No	3
			CVE-2022-38008	Remote Code Execution	Important	No	No	2
5002166	高危	Description of the security update for Office 2013: September 13, 2022 (KB5002166)	CVE-2022-37962	Remote Code Execution	Important	No	No	2
5002017	高危	Description of the security update for Visio 2013: September 13, 2022 (KB5002017)	CVE-2022-38010	Remote Code Execution	Important	No	No	2
5017500	高危	September 13, 2022-KB5017500 Cumulative Update for .NET Framework	CVE-2022-26929	Remote Code Execution	Important	No	No	2

		3.5, 4.8 and 4.8.1 for Windows 10 Version 21H2						
5002269	高危	Description of the security update for SharePoint Enterprise Server 2016: September 13, 2022 (KB5002269)	CVE-2022-38009	Remote Code Execution	Important	No	No	2
			CVE-2022-37961	Remote Code Execution	Important	No	No	3
			CVE-2022-35823	Remote Code Execution	Important	No	No	3
			CVE-2022-38008	Remote Code Execution	Important	No	No	2
5002142	高危	Description of the security update for SharePoint Enterprise Server 2016 Language Pack: September 13, 2022 (KB5002142)	CVE-2022-38008	Remote Code Execution	Important	No	No	2
5017498	高危	September 13, 2022-KB5017498 Cumulative Update for .NET Framework	CVE-2022-26929	Remote Code Execution	Important	No	No	2

		3.5, 4.8 and 4.8.1 for Windows 10, version 20H2						
5002178	高危	Description of the security update for Office 2016: September 13, 2022 (KB5002178)	CVE-2022-37962	Remote Code Execution	Important	No	No	2
5017499	高危	September 13, 2022-KB5017499 Cumulative Update for .NET Framework 3.5, 4.8 and 4.8.1 for Windows 10 Version 21H1	CVE-2022-26929	Remote Code Execution	Important	No	No	2

本月发布内容中还包括 3 个一般性更新补丁：

KBID	奇安信集团级别	详细信息
5002251	其他功能性补丁	Office 2016 更新程序
5002252	其他功能性补丁	Office 2013 更新程序
5002268	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