奇安信集团 2023 年 2 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

2023 年 2 月 15 日

目 录

文档信息

文档名称	奇安信集团 2023 年 2 月补丁库更新通告		
文档编号	Qi An Xin Group-MSPatch-2023-0201		
发布日期	2023-02-15	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:2023.02.15.1,V10版本:2023.02.15.1000)已发布，本次更新推送了37个微软安全补丁，修复了45个安全漏洞，其中6个微软官方评级为“严重(Critical)”，39个评级为“重要(Important)”，这些漏洞影响Windows、.NET Framework 、Office等产品。

第2章 重点关注补丁

本月有 16 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
5022874	CVE-2023-21818	Denial of Service	Important	No	No	Exploitation More Likely
5022872						
5022840						
5022893						
5022899						
5022838						
5022834						
5022858						
5022895						
5022894						
5022836						
5022890						
5022903						
5022874	CVE-2023-21689	Remote Code Execution	Critical	No	No	Exploitation More Likely
5022872						
5022840						
5022899						
5022838						
5022834						
5022858						
5022895						
5022845						
5022894						
5022836						
5022903						
5022874	CVE-2023-21812	Elevation of Privilege	Important	No	No	Exploitation More Likely
5022872						
5022840						

5022893						
5022899						
5022838						
5022834						
5022858						
5022895						
5022845						
5022894						
5022836						
5022890						
5022903						
5022874	CVE-2023-21692	Remote Code Execution	Critical	No	No	Exploitation More Likely
5022872						
5022840						
5022893						
5022899						
5022838						
5022834						
5022858						
5022895						
5022845						
5022894						
5022836						
5022890						
5022903						
5022874	CVE-2023-21690	Remote Code Execution	Critical	No	No	Exploitation More Likely
5022872						
5022840						
5022899						
5022838						
5022834						
5022858						
5022895						
5022845						
5022894						
5022836						
5022903						
5022874	CVE-2023-23376	Elevation of Privilege	Important	No	Yes	Exploitation Detected
5022872						
5022840						
5022893						

5022899						
5022838						
5022834						
5022858						
5022895						
5022845						
5022894						
5022836						
5022890						
5022903						
5022874	CVE-2023-21688	Elevation of Privilege	Important	No	No	Exploitation More Likely
5022872						
5022840						
5022893						
5022899						
5022838						
5022834						
5022858						
5022895						
5022845						
5022894						
5022836						
5022890						
5022903						
5022874	CVE-2023-21823	Elevation of Privilege	Important	No	Yes	Exploitation Detected
5022872						
5022840						
5022893						
5022899						
5022838						
5022834						
5022858						
5022895						
5022845						
5022894						
5022836						
5022890						
5022903						
5022874	CVE-2023-21822	Elevation of Privilege	Important	No	No	Exploitation More Likely
5022872						
5022840						

5022893						
5022899						
5022838						
5022834						
5022858						
5022895						
5022845						
5022894						
5022836						
5022890						
5022903						
5023038	CVE-2023-21706	Remote Code Execution	Important	No	No	Exploitation More Likely
5023038	CVE-2023-21707	Remote Code Execution	Important	No	No	Exploitation More Likely
5023038	CVE-2023-21529	Remote Code Execution	Important	No	No	Exploitation More Likely
5002325	CVE-2023-21716	Remote Code Execution	Critical	No	No	Exploitation Less Likely
5002313						
5002323						
5002316						
5002312						
5002347						
5022734	CVE-2023-21808	Remote Code Execution	Critical	No	No	Exploitation Less Likely
5022730						
5022728						
5022731						
5022503						
5022729						
5022783						
5022838						
5022782						
5022858						
5022497						
5022786						
5022785						
5022727						
5022784						

5022840	CVE-2023-21819	Denial of Service	Important	No	No	Exploitation More Likely
5022834						
5022836						
5022840	CVE-2023-21803	Remote Code Execution	Critical	No	No	Exploitation Less Likely
5022893						
5022838						
5022834						
5022858						
5022890						

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
5022874	高危	February 14, 2023—KB5022874 (Security-only update) - Microsoft Support for Windows Server 2008 R2 Enterprise ESU,Windows Server 2008 R2 Standard ESU,Windows Server 2008 R2 Datacenter ESU,Windows Embedded Standard	CVE-2023-21818	Denial of Service	Important	No	No	1
			CVE-2023-21689	Remote Code Execution	Critical	No	No	1
			CVE-2023-21694	Remote Code Execution	Important	No	No	2
			CVE-2023-21812	Elevation of Privilege	Important	No	No	1
			CVE-2023-21816	Denial of Service	Important	No	No	2
			CVE-2023-21817	Elevation of Privilege	Important	No	No	2
			CVE-2023-21801	Remote Code Execution	Important	No	No	2
			CVE-2023-21695	Remote Code Execution	Important	No	No	2
			CVE-2023-21692	Remote Code Execution	Critical	No	No	1
			CVE-2023-21690	Remote Code Execution	Critical	No	No	1

		7 ESU,Windows Embedded POSReady 7 ESU	CVE-2023-23376	Elevation of Privilege	Important	No	Yes	0
			CVE-2023-21700	Denial of Service	Important	No	No	2
			CVE-2023-21685	Remote Code Execution	Important	No	No	2
			CVE-2023-21799	Remote Code Execution	Important	No	No	2
			CVE-2023-21820	Remote Code Execution	Important	No	No	2
			CVE-2023-21798	Remote Code Execution	Important	No	No	2
			CVE-2023-21688	Elevation of Privilege	Important	No	No	1
			CVE-2023-21811	Denial of Service	Important	No	No	2
			CVE-2023-21691	Information Disclosure	Important	No	No	2
			CVE-2023-21693	Information Disclosure	Important	No	No	2
			CVE-2023-21797	Remote Code Execution	Important	No	No	2
			CVE-2023-21701	Denial of Service	Important	No	No	2
			CVE-2023-21697	Information Disclosure	Important	No	No	2
			CVE-2023-21686	Remote Code Execution	Important	No	No	2

			CVE-2023-21699	Information Disclosure	Important	No	No	2
			CVE-2023-21823	Elevation of Privilege	Important	No	Yes	0
			CVE-2023-21822	Elevation of Privilege	Important	No	No	1
			CVE-2023-21805	Remote Code Execution	Important	No	No	2
			CVE-2023-21800	Elevation of Privilege	Important	No	No	2
			CVE-2023-21684	Remote Code Execution	Important	No	No	2
			CVE-2023-21802	Remote Code Execution	Important	No	No	2
			CVE-2023-21813	Denial of Service	Important	No	No	2
			CVE-2023-21702	Denial of Service	Important	No	No	2
5022872	高危	February 14, 2023—KB5022872 (Monthly Rollup) - Microsoft Support for Windows Server 2008 R2 Enterprise ESU,Windows Server	CVE-2023-21818	Denial of Service	Important	No	No	1
			CVE-2023-21689	Remote Code Execution	Critical	No	No	1
			CVE-2023-21694	Remote Code Execution	Important	No	No	2
			CVE-2023-21812	Elevation of Privilege	Important	No	No	1
			CVE-2023-21816	Denial of Service	Important	No	No	2
			CVE-2023-21817	Elevation of Privilege	Important	No	No	2

		2008 R2 Standard ESU,Windows Server 2008 R2 Datacenter ESU,Windows Embedded Standard 7 ESU,Windows Embedded POSReady 7 ESU	CVE-2023-21801	Remote Code Execution	Important	No	No	2
			CVE-2023-21695	Remote Code Execution	Important	No	No	2
			CVE-2023-21692	Remote Code Execution	Critical	No	No	1
			CVE-2023-21690	Remote Code Execution	Critical	No	No	1
			CVE-2023-23376	Elevation of Privilege	Important	No	Yes	0
			CVE-2023-21700	Denial of Service	Important	No	No	2
			CVE-2023-21685	Remote Code Execution	Important	No	No	2
			CVE-2023-21799	Remote Code Execution	Important	No	No	2
			CVE-2023-21820	Remote Code Execution	Important	No	No	2
			CVE-2023-21798	Remote Code Execution	Important	No	No	2
			CVE-2023-21688	Elevation of Privilege	Important	No	No	1
			CVE-2023-21811	Denial of Service	Important	No	No	2
			CVE-2023-21691	Information Disclosure	Important	No	No	2
			CVE-2023-21693	Information Disclosure	Important	No	No	2

			CVE-2023-21797	Remote Code Execution	Important	No	No	2
			CVE-2023-21701	Denial of Service	Important	No	No	2
			CVE-2023-21697	Information Disclosure	Important	No	No	2
			CVE-2023-21686	Remote Code Execution	Important	No	No	2
			CVE-2023-21699	Information Disclosure	Important	No	No	2
			CVE-2023-21823	Elevation of Privilege	Important	No	Yes	0
			CVE-2023-21822	Elevation of Privilege	Important	No	No	1
			CVE-2023-21800	Elevation of Privilege	Important	No	No	2
			CVE-2023-21684	Remote Code Execution	Important	No	No	2
			CVE-2023-21802	Remote Code Execution	Important	No	No	2
			CVE-2023-21813	Denial of Service	Important	No	No	2
			CVE-2023-21702	Denial of Service	Important	No	No	2
5022840	高危	February 14, 2023—KB5022840 (OS Build	CVE-2023-21818	Denial of Service	Important	No	No	1
			CVE-2023-21689	Remote Code Execution	Critical	No	No	1

		17763.4010) - Microsoft Support for Win 10 Ent LTSC v2019,Win 10 IoT Ent LTSC v2019,Windows 10 IoT Core 2019 LTSC,Windows Server 2019	CVE-2023-21804	Elevation of Privilege	Important	No	No	2
			CVE-2023-21694	Remote Code Execution	Important	No	No	2
			CVE-2023-21812	Elevation of Privilege	Important	No	No	1
			CVE-2023-21816	Denial of Service	Important	No	No	2
			CVE-2023-21817	Elevation of Privilege	Important	No	No	2
			CVE-2023-21801	Remote Code Execution	Important	No	No	2
			CVE-2023-21695	Remote Code Execution	Important	No	No	2
			CVE-2023-21692	Remote Code Execution	Critical	No	No	1
			CVE-2023-21690	Remote Code Execution	Critical	No	No	1
			CVE-2023-23376	Elevation of Privilege	Important	No	Yes	0
			CVE-2023-21700	Denial of Service	Important	No	No	2
			CVE-2023-21685	Remote Code Execution	Important	No	No	2
			CVE-2023-21819	Denial of Service	Important	No	No	1
			CVE-2023-21803	Remote Code Execution	Critical	No	No	2
			CVE-2023-21799	Remote Code Execution	Important	No	No	2

			CVE-2023-21820	Remote Code Execution	Important	No	No	2
			CVE-2023-21798	Remote Code Execution	Important	No	No	2
			CVE-2023-21688	Elevation of Privilege	Important	No	No	1
			CVE-2023-21811	Denial of Service	Important	No	No	2
			CVE-2023-21691	Information Disclosure	Important	No	No	2
			CVE-2023-21693	Information Disclosure	Important	No	No	2
			CVE-2023-21797	Remote Code Execution	Important	No	No	2
			CVE-2023-21701	Denial of Service	Important	No	No	2
			CVE-2023-21697	Information Disclosure	Important	No	No	2
			CVE-2023-21686	Remote Code Execution	Important	No	No	2
			CVE-2023-21699	Information Disclosure	Important	No	No	2
			CVE-2023-21823	Elevation of Privilege	Important	No	Yes	0
			CVE-2023-21822	Elevation of Privilege	Important	No	No	1

			CVE-2023-21805	Remote Code Execution	Important	No	No	2
			CVE-2023-21684	Remote Code Execution	Important	No	No	2
			CVE-2023-21802	Remote Code Execution	Important	No	No	2
			CVE-2023-21813	Denial of Service	Important	No	No	2
			CVE-2023-21702	Denial of Service	Important	No	No	2
5022893	高危	February 14, 2023—KB5022893 (Security-only update) - Microsoft Support for Windows Server 2008 Datacenter ESU,Windows Server 2008 Standard ESU,Windows Server 2008 Enterprise ESU	CVE-2023-21818	Denial of Service	Important	No	No	1
			CVE-2023-21694	Remote Code Execution	Important	No	No	2
			CVE-2023-21812	Elevation of Privilege	Important	No	No	1
			CVE-2023-21816	Denial of Service	Important	No	No	2
			CVE-2023-21817	Elevation of Privilege	Important	No	No	2
			CVE-2023-21801	Remote Code Execution	Important	No	No	2
			CVE-2023-21695	Remote Code Execution	Important	No	No	2
			CVE-2023-21692	Remote Code Execution	Critical	No	No	1
			CVE-2023-23376	Elevation of Privilege	Important	No	Yes	0
			CVE-2023-21700	Denial of Service	Important	No	No	2

			CVE-2023-21685	Remote Code Execution	Important	No	No	2
			CVE-2023-21803	Remote Code Execution	Critical	No	No	2
			CVE-2023-21799	Remote Code Execution	Important	No	No	2
			CVE-2023-21820	Remote Code Execution	Important	No	No	2
			CVE-2023-21798	Remote Code Execution	Important	No	No	2
			CVE-2023-21688	Elevation of Privilege	Important	No	No	1
			CVE-2023-21811	Denial of Service	Important	No	No	2
			CVE-2023-21691	Information Disclosure	Important	No	No	2
			CVE-2023-21693	Information Disclosure	Important	No	No	2
			CVE-2023-21797	Remote Code Execution	Important	No	No	2
			CVE-2023-21701	Denial of Service	Important	No	No	2
			CVE-2023-21697	Information Disclosure	Important	No	No	2
			CVE-2023-21686	Remote Code Execution	Important	No	No	2
			CVE-2023-21699	Information	Important	No	No	2

				Disclosure				
			CVE-2023-21823	Elevation of Privilege	Important	No	Yes	0
			CVE-2023-21822	Elevation of Privilege	Important	No	No	1
			CVE-2023-21805	Remote Code Execution	Important	No	No	2
			CVE-2023-21800	Elevation of Privilege	Important	No	No	2
			CVE-2023-21684	Remote Code Execution	Important	No	No	2
			CVE-2023-21802	Remote Code Execution	Important	No	No	2
			CVE-2023-21813	Denial of Service	Important	No	No	2
			CVE-2023-21702	Denial of Service	Important	No	No	2
5022899	高危	February 14, 2023—KB5022899 (Monthly Rollup) - Microsoft Support for Windows Server 2012 R2,Windows Embedded 8.1	CVE-2023-21818	Denial of Service	Important	No	No	1
			CVE-2023-21689	Remote Code Execution	Critical	No	No	1
			CVE-2023-21804	Elevation of Privilege	Important	No	No	2
			CVE-2023-21694	Remote Code Execution	Important	No	No	2
			CVE-2023-21812	Elevation of Privilege	Important	No	No	1
			CVE-2023-21816	Denial of Service	Important	No	No	2

		Industry Enterprise,Windows Embedded 8.1 Industry Pro	CVE-2023-21817	Elevation of Privilege	Important	No	No	2
			CVE-2023-21801	Remote Code Execution	Important	No	No	2
			CVE-2023-21695	Remote Code Execution	Important	No	No	2
			CVE-2023-21692	Remote Code Execution	Critical	No	No	1
			CVE-2023-21690	Remote Code Execution	Critical	No	No	1
			CVE-2023-23376	Elevation of Privilege	Important	No	Yes	0
			CVE-2023-21700	Denial of Service	Important	No	No	2
			CVE-2023-21685	Remote Code Execution	Important	No	No	2
			CVE-2023-21799	Remote Code Execution	Important	No	No	2
			CVE-2023-21820	Remote Code Execution	Important	No	No	2
			CVE-2023-21798	Remote Code Execution	Important	No	No	2
			CVE-2023-21688	Elevation of Privilege	Important	No	No	1
			CVE-2023-21811	Denial of Service	Important	No	No	2
			CVE-2023-21691	Information Disclosure	Important	No	No	2

			CVE-2023-21693	Information Disclosure	Important	No	No	2
			CVE-2023-21797	Remote Code Execution	Important	No	No	2
			CVE-2023-21701	Denial of Service	Important	No	No	2
			CVE-2023-21697	Information Disclosure	Important	No	No	2
			CVE-2023-21686	Remote Code Execution	Important	No	No	2
			CVE-2023-21699	Information Disclosure	Important	No	No	2
			CVE-2023-21823	Elevation of Privilege	Important	No	Yes	0
			CVE-2023-21822	Elevation of Privilege	Important	No	No	1
			CVE-2023-21684	Remote Code Execution	Important	No	No	2
			CVE-2023-21802	Remote Code Execution	Important	No	No	2
			CVE-2023-21813	Denial of Service	Important	No	No	2
			CVE-2023-21702	Denial of Service	Important	No	No	2
5022838	高危	February 14, 2023—KB5022838 (OS Build	CVE-2023-21818	Denial of Service	Important	No	No	1
			CVE-2023-21689	Remote Code Execution	Critical	No	No	1

		14393.5717) - Microsoft Support for Windows 10, version 1607, all editions, Windows Server 2016, all editions	CVE-2023-21808	Remote Code Execution	Critical	No	No	2
			CVE-2023-21804	Elevation of Privilege	Important	No	No	2
			CVE-2023-21694	Remote Code Execution	Important	No	No	2
			CVE-2023-21812	Elevation of Privilege	Important	No	No	1
			CVE-2023-21816	Denial of Service	Important	No	No	2
			CVE-2023-21817	Elevation of Privilege	Important	No	No	2
			CVE-2023-21801	Remote Code Execution	Important	No	No	2
			CVE-2023-21695	Remote Code Execution	Important	No	No	2
			CVE-2023-21692	Remote Code Execution	Critical	No	No	1
			CVE-2023-21690	Remote Code Execution	Critical	No	No	1
			CVE-2023-23376	Elevation of Privilege	Important	No	Yes	0
			CVE-2023-21722	Denial of Service	Important	No	No	2
			CVE-2023-21700	Denial of Service	Important	No	No	2
			CVE-2023-21685	Remote Code Execution	Important	No	No	2
			CVE-2023-21803	Remote Code Execution	Critical	No	No	2

			CVE-2023-21799	Remote Code Execution	Important	No	No	2
			CVE-2023-21820	Remote Code Execution	Important	No	No	2
			CVE-2023-21798	Remote Code Execution	Important	No	No	2
			CVE-2023-21688	Elevation of Privilege	Important	No	No	1
			CVE-2023-21811	Denial of Service	Important	No	No	2
			CVE-2023-21691	Information Disclosure	Important	No	No	2
			CVE-2023-21693	Information Disclosure	Important	No	No	2
			CVE-2023-21797	Remote Code Execution	Important	No	No	2
			CVE-2023-21701	Denial of Service	Important	No	No	2
			CVE-2023-21697	Information Disclosure	Important	No	No	2
			CVE-2023-21686	Remote Code Execution	Important	No	No	2
			CVE-2023-21699	Information Disclosure	Important	No	No	2
			CVE-2023-21823	Elevation of Privilege	Important	No	Yes	0

			CVE-2023-21822	Elevation of Privilege	Important	No	No	1
			CVE-2023-21805	Remote Code Execution	Important	No	No	2
			CVE-2023-21684	Remote Code Execution	Important	No	No	2
			CVE-2023-21802	Remote Code Execution	Important	No	No	2
			CVE-2023-21813	Denial of Service	Important	No	No	2
			CVE-2023-21702	Denial of Service	Important	No	No	2
5022834	高危	February 14, 2023—KB5022834 (OS Builds 19042.2604, 19044.2604, and 19045.2604) - Microsoft Support for Windows 10 Enterprise Multi-Session, version 20H2, Windows 10 Enterprise and	CVE-2023-21818	Denial of Service	Important	No	No	1
			CVE-2023-21689	Remote Code Execution	Critical	No	No	1
			CVE-2023-21804	Elevation of Privilege	Important	No	No	2
			CVE-2023-21694	Remote Code Execution	Important	No	No	2
			CVE-2023-21812	Elevation of Privilege	Important	No	No	1
			CVE-2023-21816	Denial of Service	Important	No	No	2
			CVE-2023-21817	Elevation of Privilege	Important	No	No	2
			CVE-2023-21801	Remote Code Execution	Important	No	No	2
			CVE-2023-21695	Remote Code Execution	Important	No	No	2

		Education, version 20H2,Windows 10 IoT Enterprise, version 20H2,Windows 10 on Surface Hub,Windows 10, version 21H2, all editions, Windows 10, version 22H2, all editions	CVE-2023-21692	Remote Code Execution	Critical	No	No	1
			CVE-2023-21690	Remote Code Execution	Critical	No	No	1
			CVE-2023-23376	Elevation of Privilege	Important	No	Yes	0
			CVE-2023-21700	Denial of Service	Important	No	No	2
			CVE-2023-21685	Remote Code Execution	Important	No	No	2
			CVE-2023-21819	Denial of Service	Important	No	No	1
			CVE-2023-21803	Remote Code Execution	Critical	No	No	2
			CVE-2023-21799	Remote Code Execution	Important	No	No	2
			CVE-2023-21820	Remote Code Execution	Important	No	No	2
			CVE-2023-21798	Remote Code Execution	Important	No	No	2
			CVE-2023-21688	Elevation of Privilege	Important	No	No	1
			CVE-2023-21811	Denial of Service	Important	No	No	2
			CVE-2023-21691	Information Disclosure	Important	No	No	2
			CVE-2023-21693	Information Disclosure	Important	No	No	2

			CVE-2023-21797	Remote Code Execution	Important	No	No	2
			CVE-2023-21701	Denial of Service	Important	No	No	2
			CVE-2023-21697	Information Disclosure	Important	No	No	2
			CVE-2023-21686	Remote Code Execution	Important	No	No	2
			CVE-2023-21699	Information Disclosure	Important	No	No	2
			CVE-2023-21823	Elevation of Privilege	Important	No	Yes	0
			CVE-2023-21822	Elevation of Privilege	Important	No	No	1
			CVE-2023-21805	Remote Code Execution	Important	No	No	2
			CVE-2023-21684	Remote Code Execution	Important	No	No	2
			CVE-2023-21802	Remote Code Execution	Important	No	No	2
			CVE-2023-21813	Denial of Service	Important	No	No	2
			CVE-2023-21702	Denial of Service	Important	No	No	2
5022858	高危	February 14, 2023—KB5022858 (OS Build	CVE-2023-21818	Denial of Service	Important	No	No	1
			CVE-2023-21689	Remote Code Execution	Critical	No	No	1

		10240.19747) - Microsoft Support for Windows 10	CVE-2023-21808	Remote Code Execution	Critical	No	No	2
			CVE-2023-21804	Elevation of Privilege	Important	No	No	2
			CVE-2023-21694	Remote Code Execution	Important	No	No	2
			CVE-2023-21812	Elevation of Privilege	Important	No	No	1
			CVE-2023-21816	Denial of Service	Important	No	No	2
			CVE-2023-21817	Elevation of Privilege	Important	No	No	2
			CVE-2023-21801	Remote Code Execution	Important	No	No	2
			CVE-2023-21695	Remote Code Execution	Important	No	No	2
			CVE-2023-21692	Remote Code Execution	Critical	No	No	1
			CVE-2023-21690	Remote Code Execution	Critical	No	No	1
			CVE-2023-23376	Elevation of Privilege	Important	No	Yes	0
			CVE-2023-21722	Denial of Service	Important	No	No	2
			CVE-2023-21700	Denial of Service	Important	No	No	2
			CVE-2023-21685	Remote Code Execution	Important	No	No	2
			CVE-2023-21803	Remote Code Execution	Critical	No	No	2

			CVE-2023-21799	Remote Code Execution	Important	No	No	2
			CVE-2023-21820	Remote Code Execution	Important	No	No	2
			CVE-2023-21798	Remote Code Execution	Important	No	No	2
			CVE-2023-21688	Elevation of Privilege	Important	No	No	1
			CVE-2023-21811	Denial of Service	Important	No	No	2
			CVE-2023-21691	Information Disclosure	Important	No	No	2
			CVE-2023-21693	Information Disclosure	Important	No	No	2
			CVE-2023-21797	Remote Code Execution	Important	No	No	2
			CVE-2023-21701	Denial of Service	Important	No	No	2
			CVE-2023-21697	Information Disclosure	Important	No	No	2
			CVE-2023-21686	Remote Code Execution	Important	No	No	2
			CVE-2023-21699	Information Disclosure	Important	No	No	2
			CVE-2023-21823	Elevation of Privilege	Important	No	Yes	0

			CVE-2023-21822	Elevation of Privilege	Important	No	No	1
			CVE-2023-21805	Remote Code Execution	Important	No	No	2
			CVE-2023-21684	Remote Code Execution	Important	No	No	2
			CVE-2023-21802	Remote Code Execution	Important	No	No	2
			CVE-2023-21813	Denial of Service	Important	No	No	2
			CVE-2023-21702	Denial of Service	Important	No	No	2
5022895	高危	February 14, 2023—KB5022895 (Security-only update) - Microsoft Support for Windows Server 2012, Windows Embedded 8 Standard	CVE-2023-21818	Denial of Service	Important	No	No	1
			CVE-2023-21689	Remote Code Execution	Critical	No	No	1
			CVE-2023-21804	Elevation of Privilege	Important	No	No	2
			CVE-2023-21694	Remote Code Execution	Important	No	No	2
			CVE-2023-21812	Elevation of Privilege	Important	No	No	1
			CVE-2023-21816	Denial of Service	Important	No	No	2
			CVE-2023-21817	Elevation of Privilege	Important	No	No	2
			CVE-2023-21801	Remote Code Execution	Important	No	No	2
			CVE-2023-21695	Remote Code Execution	Important	No	No	2

			CVE-2023-21692	Remote Code Execution	Critical	No	No	1
			CVE-2023-21690	Remote Code Execution	Critical	No	No	1
			CVE-2023-23376	Elevation of Privilege	Important	No	Yes	0
			CVE-2023-21700	Denial of Service	Important	No	No	2
			CVE-2023-21685	Remote Code Execution	Important	No	No	2
			CVE-2023-21799	Remote Code Execution	Important	No	No	2
			CVE-2023-21820	Remote Code Execution	Important	No	No	2
			CVE-2023-21798	Remote Code Execution	Important	No	No	2
			CVE-2023-21688	Elevation of Privilege	Important	No	No	1
			CVE-2023-21811	Denial of Service	Important	No	No	2
			CVE-2023-21691	Information Disclosure	Important	No	No	2
			CVE-2023-21693	Information Disclosure	Important	No	No	2
			CVE-2023-21797	Remote Code Execution	Important	No	No	2
			CVE-2023-21701	Denial of Service	Important	No	No	2

			CVE-2023-21697	Information Disclosure	Important	No	No	2
			CVE-2023-21686	Remote Code Execution	Important	No	No	2
			CVE-2023-21699	Information Disclosure	Important	No	No	2
			CVE-2023-21823	Elevation of Privilege	Important	No	Yes	0
			CVE-2023-21822	Elevation of Privilege	Important	No	No	1
			CVE-2023-21805	Remote Code Execution	Important	No	No	2
			CVE-2023-21684	Remote Code Execution	Important	No	No	2
			CVE-2023-21802	Remote Code Execution	Important	No	No	2
			CVE-2023-21813	Denial of Service	Important	No	No	2
			CVE-2023-21702	Denial of Service	Important	No	No	2
5022845	高危	February 14, 2023—KB5022845 (OS Build 22621.1265) - Microsoft Support for	CVE-2023-21689	Remote Code Execution	Critical	No	No	1
			CVE-2023-21687	Information Disclosure	Important	No	No	2
			CVE-2023-21804	Elevation of Privilege	Important	No	No	2

		Windows 11 version 22H2, all editions	CVE-2023-21694	Remote Code Execution	Important	No	No	2
			CVE-2023-21812	Elevation of Privilege	Important	No	No	1
			CVE-2023-21816	Denial of Service	Important	No	No	2
			CVE-2023-21817	Elevation of Privilege	Important	No	No	2
			CVE-2023-21801	Remote Code Execution	Important	No	No	2
			CVE-2023-21695	Remote Code Execution	Important	No	No	2
			CVE-2023-21692	Remote Code Execution	Critical	No	No	1
			CVE-2023-21690	Remote Code Execution	Critical	No	No	1
			CVE-2023-23376	Elevation of Privilege	Important	No	Yes	0
			CVE-2023-21700	Denial of Service	Important	No	No	2
			CVE-2023-21685	Remote Code Execution	Important	No	No	2
			CVE-2023-21799	Remote Code Execution	Important	No	No	2
			CVE-2023-21820	Remote Code Execution	Important	No	No	2
			CVE-2023-21798	Remote Code Execution	Important	No	No	2

			CVE-2023-21688	Elevation of Privilege	Important	No	No	1
			CVE-2023-21811	Denial of Service	Important	No	No	2
			CVE-2023-21691	Information Disclosure	Important	No	No	2
			CVE-2023-21693	Information Disclosure	Important	No	No	2
			CVE-2023-21797	Remote Code Execution	Important	No	No	2
			CVE-2023-21701	Denial of Service	Important	No	No	2
			CVE-2023-21686	Remote Code Execution	Important	No	No	2
			CVE-2023-21823	Elevation of Privilege	Important	No	Yes	0
			CVE-2023-21822	Elevation of Privilege	Important	No	No	1
			CVE-2023-21805	Remote Code Execution	Important	No	No	2
			CVE-2023-21684	Remote Code Execution	Important	No	No	2
			CVE-2023-21802	Remote Code Execution	Important	No	No	2
			CVE-2023-21813	Denial of Service	Important	No	No	2
			CVE-2023-21702	Denial of Service	Important	No	No	2
5022894	高危	February 14,	CVE-2023-21818	Denial of Service	Important	No	No	1

		2023—KB5022894 (Security-only update) - Microsoft Support for Windows Server 2012 R2,Windows Embedded 8.1 Industry Enterprise,Windows Embedded 8.1 Industry Pro	CVE-2023-21689	Remote Code Execution	Critical	No	No	1
			CVE-2023-21804	Elevation of Privilege	Important	No	No	2
			CVE-2023-21694	Remote Code Execution	Important	No	No	2
			CVE-2023-21812	Elevation of Privilege	Important	No	No	1
			CVE-2023-21816	Denial of Service	Important	No	No	2
			CVE-2023-21817	Elevation of Privilege	Important	No	No	2
			CVE-2023-21801	Remote Code Execution	Important	No	No	2
			CVE-2023-21695	Remote Code Execution	Important	No	No	2
			CVE-2023-21692	Remote Code Execution	Critical	No	No	1
			CVE-2023-21690	Remote Code Execution	Critical	No	No	1
			CVE-2023-23376	Elevation of Privilege	Important	No	Yes	0
			CVE-2023-21700	Denial of Service	Important	No	No	2
			CVE-2023-21685	Remote Code Execution	Important	No	No	2
			CVE-2023-21799	Remote Code Execution	Important	No	No	2

			CVE-2023-21820	Remote Code Execution	Important	No	No	2
			CVE-2023-21798	Remote Code Execution	Important	No	No	2
			CVE-2023-21688	Elevation of Privilege	Important	No	No	1
			CVE-2023-21811	Denial of Service	Important	No	No	2
			CVE-2023-21691	Information Disclosure	Important	No	No	2
			CVE-2023-21693	Information Disclosure	Important	No	No	2
			CVE-2023-21797	Remote Code Execution	Important	No	No	2
			CVE-2023-21701	Denial of Service	Important	No	No	2
			CVE-2023-21697	Information Disclosure	Important	No	No	2
			CVE-2023-21686	Remote Code Execution	Important	No	No	2
			CVE-2023-21699	Information Disclosure	Important	No	No	2
			CVE-2023-21823	Elevation of Privilege	Important	No	Yes	0
			CVE-2023-21822	Elevation of Privilege	Important	No	No	1

			CVE-2023-21805	Remote Code Execution	Important	No	No	2
			CVE-2023-21684	Remote Code Execution	Important	No	No	2
			CVE-2023-21802	Remote Code Execution	Important	No	No	2
			CVE-2023-21813	Denial of Service	Important	No	No	2
			CVE-2023-21702	Denial of Service	Important	No	No	2
5022836	高危	February 14, 2023—KB5022836 (OS Build 22000.1574) - Microsoft Support for Windows 11 version 21H2, all editions	CVE-2023-21818	Denial of Service	Important	No	No	1
			CVE-2023-21689	Remote Code Execution	Critical	No	No	1
			CVE-2023-21687	Information Disclosure	Important	No	No	2
			CVE-2023-21804	Elevation of Privilege	Important	No	No	2
			CVE-2023-21694	Remote Code Execution	Important	No	No	2
			CVE-2023-21812	Elevation of Privilege	Important	No	No	1
			CVE-2023-21816	Denial of Service	Important	No	No	2
			CVE-2023-21817	Elevation of Privilege	Important	No	No	2
			CVE-2023-21801	Remote Code Execution	Important	No	No	2
			CVE-2023-21695	Remote Code Execution	Important	No	No	2

			CVE-2023-21692	Remote Code Execution	Critical	No	No	1
			CVE-2023-21690	Remote Code Execution	Critical	No	No	1
			CVE-2023-23376	Elevation of Privilege	Important	No	Yes	0
			CVE-2023-21700	Denial of Service	Important	No	No	2
			CVE-2023-21685	Remote Code Execution	Important	No	No	2
			CVE-2023-21819	Denial of Service	Important	No	No	1
			CVE-2023-21799	Remote Code Execution	Important	No	No	2
			CVE-2023-21820	Remote Code Execution	Important	No	No	2
			CVE-2023-21798	Remote Code Execution	Important	No	No	2
			CVE-2023-21688	Elevation of Privilege	Important	No	No	1
			CVE-2023-21811	Denial of Service	Important	No	No	2
			CVE-2023-21691	Information Disclosure	Important	No	No	2
			CVE-2023-21693	Information Disclosure	Important	No	No	2
			CVE-2023-21797	Remote Code Execution	Important	No	No	2

			CVE-2023-21701	Denial of Service	Important	No	No	2
			CVE-2023-21686	Remote Code Execution	Important	No	No	2
			CVE-2023-21823	Elevation of Privilege	Important	No	Yes	0
			CVE-2023-21822	Elevation of Privilege	Important	No	No	1
			CVE-2023-21805	Remote Code Execution	Important	No	No	2
			CVE-2023-21684	Remote Code Execution	Important	No	No	2
			CVE-2023-21802	Remote Code Execution	Important	No	No	2
			CVE-2023-21813	Denial of Service	Important	No	No	2
			CVE-2023-21702	Denial of Service	Important	No	No	2
5022890	高危	February 14, 2023—KB5022890 (Monthly Rollup) - Microsoft Support for Windows Server 2008 Datacenter ESU,Windows Server	CVE-2023-21818	Denial of Service	Important	No	No	1
			CVE-2023-21694	Remote Code Execution	Important	No	No	2
			CVE-2023-21812	Elevation of Privilege	Important	No	No	1
			CVE-2023-21816	Denial of Service	Important	No	No	2
			CVE-2023-21817	Elevation of Privilege	Important	No	No	2
			CVE-2023-21801	Remote Code Execution	Important	No	No	2

		2008 Standard ESU,Windows Server 2008 Enterprise ESU	CVE-2023-21695	Remote Code Execution	Important	No	No	2
			CVE-2023-21692	Remote Code Execution	Critical	No	No	1
			CVE-2023-23376	Elevation of Privilege	Important	No	Yes	0
			CVE-2023-21700	Denial of Service	Important	No	No	2
			CVE-2023-21685	Remote Code Execution	Important	No	No	2
			CVE-2023-21803	Remote Code Execution	Critical	No	No	2
			CVE-2023-21799	Remote Code Execution	Important	No	No	2
			CVE-2023-21820	Remote Code Execution	Important	No	No	2
			CVE-2023-21798	Remote Code Execution	Important	No	No	2
			CVE-2023-21688	Elevation of Privilege	Important	No	No	1
			CVE-2023-21811	Denial of Service	Important	No	No	2
			CVE-2023-21691	Information Disclosure	Important	No	No	2
			CVE-2023-21693	Information Disclosure	Important	No	No	2
			CVE-2023-21797	Remote Code Execution	Important	No	No	2

			CVE-2023-21701	Denial of Service	Important	No	No	2
			CVE-2023-21697	Information Disclosure	Important	No	No	2
			CVE-2023-21686	Remote Code Execution	Important	No	No	2
			CVE-2023-21699	Information Disclosure	Important	No	No	2
			CVE-2023-21823	Elevation of Privilege	Important	No	Yes	0
			CVE-2023-21822	Elevation of Privilege	Important	No	No	1
			CVE-2023-21805	Remote Code Execution	Important	No	No	2
			CVE-2023-21800	Elevation of Privilege	Important	No	No	2
			CVE-2023-21684	Remote Code Execution	Important	No	No	2
			CVE-2023-21802	Remote Code Execution	Important	No	No	2
			CVE-2023-21813	Denial of Service	Important	No	No	2
			CVE-2023-21702	Denial of Service	Important	No	No	2
5022903	高危	February 14, 2023—KB5022903 (Monthly	CVE-2023-21818	Denial of Service	Important	No	No	1
			CVE-2023-21689	Remote Code Execution	Critical	No	No	1

		Rollup) - Microsoft Support for Windows Server 2012,Windows Embedded 8 Standard	CVE-2023-21804	Elevation of Privilege	Important	No	No	2
			CVE-2023-21694	Remote Code Execution	Important	No	No	2
			CVE-2023-21812	Elevation of Privilege	Important	No	No	1
			CVE-2023-21816	Denial of Service	Important	No	No	2
			CVE-2023-21817	Elevation of Privilege	Important	No	No	2
			CVE-2023-21801	Remote Code Execution	Important	No	No	2
			CVE-2023-21695	Remote Code Execution	Important	No	No	2
			CVE-2023-21692	Remote Code Execution	Critical	No	No	1
			CVE-2023-21690	Remote Code Execution	Critical	No	No	1
			CVE-2023-23376	Elevation of Privilege	Important	No	Yes	0
			CVE-2023-21700	Denial of Service	Important	No	No	2
			CVE-2023-21685	Remote Code Execution	Important	No	No	2
			CVE-2023-21799	Remote Code Execution	Important	No	No	2
			CVE-2023-21820	Remote Code Execution	Important	No	No	2

			CVE-2023-21798	Remote Code Execution	Important	No	No	2
			CVE-2023-21688	Elevation of Privilege	Important	No	No	1
			CVE-2023-21811	Denial of Service	Important	No	No	2
			CVE-2023-21691	Information Disclosure	Important	No	No	2
			CVE-2023-21693	Information Disclosure	Important	No	No	2
			CVE-2023-21797	Remote Code Execution	Important	No	No	2
			CVE-2023-21701	Denial of Service	Important	No	No	2
			CVE-2023-21697	Information Disclosure	Important	No	No	2
			CVE-2023-21686	Remote Code Execution	Important	No	No	2
			CVE-2023-21699	Information Disclosure	Important	No	No	2
			CVE-2023-21823	Elevation of Privilege	Important	No	Yes	0
			CVE-2023-21822	Elevation of Privilege	Important	No	No	1
			CVE-2023-21684	Remote Code Execution	Important	No	No	2

			CVE-2023-21802	Remote Code Execution	Important	No	No	2
			CVE-2023-21813	Denial of Service	Important	No	No	2
			CVE-2023-21702	Denial of Service	Important	No	No	2

本月微软发布的软件安全更新补丁共 21 个，详细列表如下：

KBID	奇安信集团级别	补丁名称	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
5023038	高危	Description of the security update for Microsoft Exchange Server 2019, 2016, and 2013: February 14, 2023 (KB5023038) - Microsoft Support	CVE-2023-21706	Remote Code Execution	Important	No	No	1
			CVE-2023-21710	Remote Code Execution	Important	No	No	2
			CVE-2023-21707	Remote Code Execution	Important	No	No	1
			CVE-2023-21529	Remote Code Execution	Important	No	No	1
5002325	高危	Description of the security update for SharePoint Enterprise	CVE-2023-21716	Remote Code Execution	Critical	No	No	2
			CVE-2023-21717	Elevation of Privilege	Important	No	No	2

		Server 2016 Language Pack: February 14, 2023 (KB5002325) - Microsoft Support						
5022734	高危	February 14, 2023-Security and Quality Rollup for .NET Framework 2.0, 3.0, 4.6.2 for Windows Server 2008 SP2 (KB5022734) - Microsoft Support	CVE-2023-21808	Remote Code Execution	Critical	No	No	2
			CVE-2023-21722	Denial of Service	Important	No	No	2
5022730	高危	February 14, 2023-KB5022730 Cumulative Update for .NET Framework 3.5, 4.8 and 4.8.1 for Windows 11, version 21H2 - Microsoft Support	CVE-2023-21808	Remote Code Execution	Critical	No	No	2
			CVE-2023-21722	Denial of Service	Important	No	No	2

5022728	高危	February 14, 2023-KB5022728 Cumulative Update for .NET Framework 3.5, 4.8 and 4.8.1 for Windows 10 Version 21H2 - Microsoft Support	CVE-2023-21808	Remote Code Execution	Critical	No	No	2
			CVE-2023-21722	Denial of Service	Important	No	No	2
5022731	高危	February 14, 2023-Security and Quality Rollup for .NET Framework 3.5.1, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Windows Embedded 7 Standard and Windows Server 2008 R2 SP1 (KB5022731) - Microsoft Support	CVE-2023-21808	Remote Code Execution	Critical	No	No	2
			CVE-2023-21722	Denial of Service	Important	No	No	2
5022503	高危	February 14, 2023-KB5022503 Cumulative Update for .NET	CVE-2023-21808	Remote Code Execution	Critical	No	No	2

		Framework 4.8 for Windows 10, version 1607 and Windows Server 2016 - Microsoft Support	CVE-2023-21722	Denial of Service	Important	No	No	2
5022729	高危	February 14, 2023-KB5022729 Cumulative Update for .NET Framework 3.5, 4.8 and 4.8.1 for Windows 10 Version 22H2 - Microsoft Support	CVE-2023-21808	Remote Code Execution	Critical	No	No	2
			CVE-2023-21722	Denial of Service	Important	No	No	2
5022783	高危	February 14, 2023-Security Only Update for .NET Framework 3.5.1, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Windows Embedded 7 Standard and Windows Server 2008 R2 SP1 (KB5022783)	CVE-2023-21808	Remote Code Execution	Critical	No	No	2
			CVE-2023-21722	Denial of Service	Important	No	No	2

		- Microsoft Support						
5002313	高危	Description of the security update for Office Web Apps Server 2013: February 14, 2023 (KB5002313) - Microsoft Support	CVE-2023-21716	Remote Code Execution	Critical	No	No	2
5002350	高危	Description of the security update for SharePoint Enterprise Server 2016: February 14, 2023 (KB5002350) - Microsoft Support	CVE-2023-21717	Elevation of Privilege	Important	No	No	2
5002323	高危	Description of the security update for Word 2016: February 14, 2023 (KB5002323) - Microsoft Support	CVE-2023-21716	Remote Code Execution	Critical	No	No	2

5022782	高危	February 14, 2023-KB5022782 Cumulative Update for .NET Framework 3.5, 4.7.2 and 4.8 for Windows 10, version 1809 and Windows Server 2019 - Microsoft Support	CVE-2023-21808	Remote Code Execution	Critical	No	No	2
			CVE-2023-21722	Denial of Service	Important	No	No	2
5022497	高危	February 14, 2023-KB5022497 Cumulative Update for .NET Framework 3.5 and 4.8.1 for Windows 11, version 22H2 - Microsoft Support	CVE-2023-21808	Remote Code Execution	Critical	No	No	2
			CVE-2023-21722	Denial of Service	Important	No	No	2
5022786	高危	February 14, 2023-Security Only Update for .NET Framework 2.0, 3.0, 4.6.2 for Windows Server 2008	CVE-2023-21808	Remote Code Execution	Critical	No	No	2
			CVE-2023-21722	Denial of Service	Important	No	No	2

		SP2 (KB5022786) - Microsoft Support						
5002316	高危	Description of the security update for Word 2013: February 14, 2023 (KB5002316) - Microsoft Support	CVE-2023-21716	Remote Code Execution	Critical	No	No	2
5022785	高危	February 14, 2023-Security Only Update for .NET Framework 3.5, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Windows Embedded 8.1 and Windows Server 2012 R2 (KB5022785) - Microsoft Support	CVE-2023-21808	Remote Code Execution	Critical	No	No	2
			CVE-2023-21722	Denial of Service	Important	No	No	2
5022727	高危	February 14, 2023-KB5022727 Cumulative Update for .NET Framework 3.5, 4.8	CVE-2023-21808	Remote Code Execution	Critical	No	No	2
			CVE-2023-21722	Denial of Service	Important	No	No	2

		and 4.8.1 for Windows 10, version 20H2 - Microsoft Support						
5002312	高危	Description of the security update for SharePoint Enterprise Server 2013: February 14, 2023 (KB5002312) - Microsoft Support	CVE-2023-21716	Remote Code Execution	Critical	No	No	2
			CVE-2023-21717	Elevation of Privilege	Important	No	No	2
5022784	高危	February 14, 2023-Security Only Update for .NET Framework 3.5, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Windows Embedded 8 Standard and Windows Server 2012 (KB5022784) - Microsoft Support	CVE-2023-21808	Remote Code Execution	Critical	No	No	2
			CVE-2023-21722	Denial of Service	Important	No	No	2

5002347	高危	Description of the security update for SharePoint Foundation 2013: February 14, 2023 (KB5002347) - Microsoft Support	CVE-2023-21716	Remote Code Execution	Critical	No	No	2
			CVE-2023-21717	Elevation of Privilege	Important	No	No	2

本月发布内容无一般性更新补丁。

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