奇安信集团 2022 年 08 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 08 月 10 日

目 录

第 1 章 安全通告 2

第 2 章 重点关注补丁 3

第 3 章 已知问题和特殊调整 11

第 4 章 漏洞补丁详细列表 12

第 5 章 参考链接 51

文档信息

文档名称	奇安信集团 2022 年 08 月补丁库更新通告		
文档编号	Qi An Xin Group-MSPatch-2022-0810		
发布日期	2022-08-10	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:2022.08.10.1,V10版本:2022.08.10.1000)已发布，本次更新推送了23个微软安全补丁，修复了69个安全漏洞，其中16个微软官方评级为“严重(Critical)”，53个评级为“重要(Important)”，这些漏洞影响产品Windows和Microsoft Office。同时推送了2个非安全office补丁。

2019年4月10日发布的天擎6.6.0.2000及以上版本支持Windows 10安全更新补丁管理，如需此功能请更新版本。

第2章 重点关注补丁

本月有 33 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
5016618 5016679 5016639 5016623 5016686 5016616 5016622 5016669 5016681 5016683 5016629 5016672 5016684 5016676	CVE-2022-34691	Elevation of Privilege	Critical	No	No	Exploitation Less Likely
5016618 5016679 5016639 5016623 5016686 5016616 5016622 5016669 5016681 5016683 5016629 5016672	CVE-2022-35744	Remote Code Execution	Critical	No	No	Exploitation Less Likely

5016684 5016676						
5016618 5016679 5016639 5016623 5016686 5016616 5016622 5016669 5016681 5016683 5016629 5016672 5016684 5016676	CVE-2022-34714	Remote Code Execution	Critical	No	No	Exploitation Less Likely
5016618 5016679 5016639 5016623 5016686 5016616 5016622 5016669 5016681 5016683 5016629 5016672 5016684 5016676	CVE-2022-35750	Elevation of Privilege	Important	No	No	Exploitation More Likely
5016618 5016639 5016623 5016616 5016622 5016681 5016683 5016629 5016672 5016684	CVE-2022-33670	Elevation of Privilege	Important	No	No	Exploitation More Likely

5016618 5016639 5016623 5016616 5016622 5016681 5016683 5016629	CVE-2022-35755	Elevation of Privilege	Important	No	No	Exploitation More Likely
5016618 5016679 5016639 5016623 5016616 5016622 5016681 5016683 5016629 5016672 5016684 5016676	CVE-2022-34713	Remote Code Execution	Important	Yes	Yes	Exploitation Detected
5016618 5016679 5016639 5016623 5016616 5016622 5016681 5016683 5016629 5016672 5016684 5016676	CVE-2022-35743	Remote Code Execution	Important	No	No	Exploitation More Likely
5016618 5016679 5012170 5016616 5016681 5016683 5016629 5016672 5016684	CVE-2022-35820	Elevation of Privilege	Important	No	No	Exploitation More Likely

5016676						
5016618 5016679 5016639 5016623 5016686 5016616 5016622 5016669 5016681 5016683 5016629 5016672 5016684 5016676	CVE-2022-35745	Remote Code Execution	Critical	No	No	Exploitation Less Likely
5016618 5016679 5016639 5016623 5016686 5016616 5016622 5016669 5016681 5016683 5016629 5016672 5016684 5016676	CVE-2022-35753	Remote Code Execution	Critical	No	No	Exploitation Less Likely
5016618 5016679 5016639 5016623 5016616 5016622 5016681 5016683 5016629 5016672 5016684 5016676	CVE-2022-35756	Elevation of Privilege	Important	No	No	Exploitation More Likely

5016618 5016679 5016639 5016623 5016686 5016616 5016622 5016669 5016681 5016683 5016629 5016672 5016684 5016676	CVE-2022-30133	Remote Code Execution	Critical	No	No	Exploitation Less Likely
5016618 5016679 5016639 5016623 5016686 5016616 5016622 5016669 5016681 5016683 5016629 5016672 5016684 5016676	CVE-2022-35767	Remote Code Execution	Critical	No	No	Exploitation Less Likely
5016618 5016679 5016639 5016623 5016686 5016616 5016622 5016669 5016681 5016683 5016629 5016672 5016684	CVE-2022-34702	Remote Code Execution	Critical	No	No	Exploitation Less Likely

5016676						
5016618 5016679 5016639 5016623 5016686 5016616 5016622 5016669 5016681 5016683 5016629 5016672 5016684 5016676	CVE-2022-35793	Elevation of Privilege	Important	No	No	Exploitation More Likely
5016618 5016679 5016639 5016623 5016686 5016616 5016622 5016669 5016681 5016683 5016629 5016672 5016684 5016676	CVE-2022-35752	Remote Code Execution	Critical	No	No	Exploitation Less Likely
5016679 5016639 5016623 5016686 5016616 5016622 5016669 5016681 5016683 5016629 5016672 5016684	CVE-2022-35751	Elevation of Privilege	Important	No	No	Exploitation More Likely

5016676						
5016639 5016623 5016616 5016622 5016629	CVE-2022-34703	Elevation of Privilege	Important	No	No	Exploitation More Likely
5016639 5016623 5016616 5016622 5016681 5016683 5016629	CVE-2022-34696	Remote Code Execution	Critical	No	No	Exploitation Less Likely
5016623 5016616 5016622 5016681 5016683 5016672 5016684	CVE-2022-35748	Denial of Service	Important	No	No	Exploitation More Likely
5016623 5016616 5016622 5016629	CVE-2022-34699	Elevation of Privilege	Important	No	No	Exploitation More Likely
5016623 5016616 5016629	CVE-2022-35794	Remote Code Execution	Critical	No	No	Exploitation Less Likely
5016623 5016616 5016622 5016629	CVE-2022-35761	Elevation of Privilege	Important	No	No	Exploitation More Likely
5016623 5016616 5016629	CVE-2022-35766	Remote Code Execution	Critical	No	No	Exploitation Less Likely
5012170 5016616 5016629	CVE-2022-34303	Security Feature Bypass	Important	No	No	Exploitation More Likely
5012170 5016616 5016629	CVE-2022-34301	Security Feature Bypass	Important	No	No	Exploitation More Likely
5012170	CVE-2022-3430	Security	Important	No	No	Exploitation

5016616 5016629	2	Feature Bypass				More Likely
5015321 5015322	CVE-2022-24477	Elevation of Privilege	Critical	No	No	Exploitation More Likely
5015321 5015322	CVE-2022-30134	Information Disclosure	Important	Yes	No	Exploitation Unlikely
5015321 5015322	CVE-2022-21980	Elevation of Privilege	Critical	No	No	Exploitation More Likely
5015321 5015322	CVE-2022-24516	Elevation of Privilege	Critical	No	No	Exploitation More Likely
5016629	CVE-2022-35804	Remote Code Execution	Critical	No	No	Exploitation More Likely

第3章 已知问题和特殊调整

本月微软发布 KB5012170 Security update for Secure Boot DBX，已调整为可选高危等级。

涉及系统：

Windows 11

Windows 10 Version 21H2

Windows 10 Version 21H1

Windows 10 Version 20H2

Windows 10 Version 1809

Windows 10 Version 1607

Windows Server 2022

Windows Server 2019

Windows Server 2016

Windows Server 2012 R2

Windows Server 2012

Windows 8.1

原因：

1 某些原始设备制造商(OEM)固件可能不允许安装此更新；

2 如果为本地 UEFI 固件配置启用了 BitLocker 组策略，配置 TPM 平台验证配置文件，并且通过策略选择了 PCR7，则可能导致更新安装失败；

3 在不兼容的系统上安装此补丁可能导致运行时错误、系统挂起，甚至无法恢复的启动失败。

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
5016639	高危	August 9, 2022 — KB5016639 (OS Build 10240.19387) for Windows 10	CVE-2022-34691	Elevation of Privilege	Critical	No	No	2
			CVE-2022-35744	Remote Code Execution	Critical	No	No	2
			CVE-2022-34714	Remote Code Execution	Critical	No	No	2
			CVE-2022-35750	Elevation of Privilege	Important	No	No	1
			CVE-2022-35754	Elevation of Privilege	Important	No	No	2
			CVE-2022-34706	Elevation of Privilege	Important	No	No	2
			CVE-2022-35758	Information Disclosure	Important	No	No	2
			CVE-2022-34703	Elevation of Privilege	Important	No	No	1
			CVE-2022-35795	Elevation of Privilege	Important	No	No	2
			CVE-2022-34701	Denial of Service	Important	No	No	2
			CVE-2022-34709	Security Feature	Important	No	No	2

				Bypass				
			CVE-2022-33670	Elevation of Privilege	Important	No	No	1
			CVE-2022-34710	Information Disclosure	Important	No	No	2
			CVE-2022-35768	Elevation of Privilege	Important	No	No	2
			CVE-2022-30144	Remote Code Execution	Important	No	No	2
			CVE-2022-35746	Elevation of Privilege	Important	No	No	2
			CVE-2022-35759	Denial of Service	Important	No	No	2
			CVE-2022-35755	Elevation of Privilege	Important	No	No	1
			CVE-2022-34713	Remote Code Execution	Important	Yes	Yes	0
			CVE-2022-35743	Remote Code Execution	Important	No	No	1
			CVE-2022-34690	Elevation of Privilege	Important	No	No	2
			CVE-2022-35747	Denial of Service	Important	No	No	2
			CVE-2022-35749	Elevation of Privilege	Important	No	No	2
			CVE-2022-35751	Elevation of Privilege	Important	No	No	1
			CVE-2022-35760	Elevation of Privilege	Important	No	No	2
			CVE-2022-35769	Denial of Service	Important	No	No	2
			CVE-2022-30194	Remote Code Execution	Important	No	No	2

			CVE-2022-35745	Remote Code Execution	Critical	No	No	2
			CVE-2022-34708	Information Disclosure	Important	No	No	2
			CVE-2022-35753	Remote Code Execution	Critical	No	No	2
			CVE-2022-35756	Elevation of Privilege	Important	No	No	1
			CVE-2022-34707	Elevation of Privilege	Important	No	No	2
			CVE-2022-30133	Remote Code Execution	Critical	No	No	2
			CVE-2022-34696	Remote Code Execution	Critical	No	No	2
			CVE-2022-35767	Remote Code Execution	Critical	No	No	2
			CVE-2022-35771	Elevation of Privilege	Important	No	No	2
			CVE-2022-34702	Remote Code Execution	Critical	No	No	2
			CVE-2022-35793	Elevation of Privilege	Important	No	No	1
			CVE-2022-35752	Remote Code Execution	Critical	No	No	2
			CVE-2022-34704	Information Disclosure	Important	No	No	2
5016679	高危	August 9, 2022 — KB5016679 (Security-only update) for Windows	CVE-2022-34691	Elevation of Privilege	Critical	No	No	2
			CVE-2022-35744	Remote Code Execution	Critical	No	No	2
			CVE-2022-34714	Remote Code Execution	Critical	No	No	2
			CVE-2022-35750	Elevation of Privilege	Important	No	No	1

		7 Enterprise ESU,Windows 7 Professional ESU,Windows 7 Ultimate ESU,Windows Server 2008 R2 Enterprise ESU,Windows Server 2008 R2 Standard ESU,Windows Server 2008 R2 Datacenter ESU,Windows Embedded Standard 7 ESU,Windows Embedded POSReady 7 ESU	CVE-2022-34706	Elevation of Privilege	Important	No	No	2
			CVE-2022-35758	Information Disclosure	Important	No	No	2
			CVE-2022-35795	Elevation of Privilege	Important	No	No	2
			CVE-2022-34701	Denial of Service	Important	No	No	2
			CVE-2022-35768	Elevation of Privilege	Important	No	No	2
			CVE-2022-35759	Denial of Service	Important	No	No	2
			CVE-2022-34713	Remote Code Execution	Important	Yes	Yes	0
			CVE-2022-35743	Remote Code Execution	Important	No	No	1
			CVE-2022-34690	Elevation of Privilege	Important	No	No	2
			CVE-2022-35747	Denial of Service	Important	No	No	2
			CVE-2022-35751	Elevation of Privilege	Important	No	No	1
			CVE-2022-35760	Elevation of Privilege	Important	No	No	2
			CVE-2022-35769	Denial of Service	Important	No	No	2
			CVE-2022-35820	Elevation of Privilege	Important	No	No	1
			CVE-2022-35745	Remote Code Execution	Critical	No	No	2
			CVE-2022-34708	Information Disclosure	Important	No	No	2
			CVE-2022-30194	Remote Code	Important	No	No	2

				Execution				
			CVE-2022-35753	Remote Code Execution	Critical	No	No	2
			CVE-2022-35756	Elevation of Privilege	Important	No	No	1
			CVE-2022-34707	Elevation of Privilege	Important	No	No	2
			CVE-2022-30133	Remote Code Execution	Critical	No	No	2
			CVE-2022-35767	Remote Code Execution	Critical	No	No	2
			CVE-2022-34702	Remote Code Execution	Critical	No	No	2
			CVE-2022-35793	Elevation of Privilege	Important	No	No	1
			CVE-2022-35752	Remote Code Execution	Critical	No	No	2
5016623	高危	August 9, 2022—KB 5016623 (OS Build 17763.3287) for Windows 10 Enterprise 2019 LTSC, Windows 10 IoT Enterprise 2019 LTSC, Windows 10 IoT Core 2019 LTSC, Win	CVE-2022-34691	Elevation of Privilege	Critical	No	No	2
			CVE-2022-30197	Information Disclosure	Important	No	No	2
			CVE-2022-35762	Elevation of Privilege	Important	No	No	2
			CVE-2022-35744	Remote Code Execution	Critical	No	No	2
			CVE-2022-34714	Remote Code Execution	Critical	No	No	2
			CVE-2022-35750	Elevation of Privilege	Important	No	No	1
			CVE-2022-35754	Elevation of Privilege	Important	No	No	2
			CVE-2022-34706	Elevation of Privilege	Important	No	No	2

		dows Server 2019	CVE-2022-35758	Information Disclosure	Important	No	No	2
			CVE-2022-35748	Denial of Service	Important	No	No	1
			CVE-2022-34703	Elevation of Privilege	Important	No	No	1
			CVE-2022-35795	Elevation of Privilege	Important	No	No	2
			CVE-2022-34701	Denial of Service	Important	No	No	2
			CVE-2022-34709	Security Feature Bypass	Important	No	No	2
			CVE-2022-33670	Elevation of Privilege	Important	No	No	1
			CVE-2022-34710	Information Disclosure	Important	No	No	2
			CVE-2022-34699	Elevation of Privilege	Important	No	No	1
			CVE-2022-35764	Elevation of Privilege	Important	No	No	2
			CVE-2022-35768	Elevation of Privilege	Important	No	No	2
			CVE-2022-30144	Remote Code Execution	Important	No	No	2
			CVE-2022-35746	Elevation of Privilege	Important	No	No	2
			CVE-2022-35759	Denial of Service	Important	No	No	2
			CVE-2022-35755	Elevation of Privilege	Important	No	No	1
			CVE-2022-34713	Remote Code	Important	Yes	Yes	0

				Execution				
			CVE-2022-35743	Remote Code Execution	Important	No	No	1
			CVE-2022-34690	Elevation of Privilege	Important	No	No	2
			CVE-2022-35747	Denial of Service	Important	No	No	2
			CVE-2022-35794	Remote Code Execution	Critical	No	No	2
			CVE-2022-34705	Elevation of Privilege	Important	No	No	2
			CVE-2022-35749	Elevation of Privilege	Important	No	No	2
			CVE-2022-35765	Elevation of Privilege	Important	No	No	2
			CVE-2022-35751	Elevation of Privilege	Important	No	No	1
			CVE-2022-35760	Elevation of Privilege	Important	No	No	2
			CVE-2022-35769	Denial of Service	Important	No	No	2
			CVE-2022-30194	Remote Code Execution	Important	No	No	2
			CVE-2022-35745	Remote Code Execution	Critical	No	No	2
			CVE-2022-34708	Information Disclosure	Important	No	No	2
			CVE-2022-35761	Elevation of Privilege	Important	No	No	1
			CVE-2022-35766	Remote Code Execution	Critical	No	No	2
			CVE-2022-35753	Remote Code Execution	Critical	No	No	2
			CVE-2022-35756	Elevation	Important	No	No	1

				of Privilege				
			CVE-2022-34707	Elevation of Privilege	Important	No	No	2
			CVE-2022-30133	Remote Code Execution	Critical	No	No	2
			CVE-2022-34696	Remote Code Execution	Critical	No	No	2
			CVE-2022-35767	Remote Code Execution	Critical	No	No	2
			CVE-2022-35771	Elevation of Privilege	Important	No	No	2
			CVE-2022-34702	Remote Code Execution	Critical	No	No	2
			CVE-2022-35793	Elevation of Privilege	Important	No	No	1
			CVE-2022-35752	Remote Code Execution	Critical	No	No	2
			CVE-2022-35763	Elevation of Privilege	Important	No	No	2
			CVE-2022-35757	Elevation of Privilege	Important	No	No	2
			CVE-2022-35792	Elevation of Privilege	Important	No	No	2
			CVE-2022-35797	Security Feature Bypass	Important	No	No	2
			CVE-2022-34704	Information Disclosure	Important	No	No	2
5016686	高危	August 9, 2022 — KB5016686 (Securit	CVE-2022-34691	Elevation of Privilege	Critical	No	No	2
			CVE-2022-35744	Remote Code Execution	Critical	No	No	2
			CVE-2022-34714	Remote Code	Critical	No	No	2

		y-only update) for Windows Server 2008 Datacenter ESU,Windows Server 2008 Standard ESU,Windows Server 2008 Enterprise ESU		Execution				
			CVE-2022-35750	Elevation of Privilege	Important	No	No	1
			CVE-2022-34706	Elevation of Privilege	Important	No	No	2
			CVE-2022-35758	Information Disclosure	Important	No	No	2
			CVE-2022-34701	Denial of Service	Important	No	No	2
			CVE-2022-35768	Elevation of Privilege	Important	No	No	2
			CVE-2022-35759	Denial of Service	Important	No	No	2
			CVE-2022-34690	Elevation of Privilege	Important	No	No	2
			CVE-2022-35747	Denial of Service	Important	No	No	2
			CVE-2022-35751	Elevation of Privilege	Important	No	No	1
			CVE-2022-35769	Denial of Service	Important	No	No	2
			CVE-2022-30194	Remote Code Execution	Important	No	No	2
			CVE-2022-35745	Remote Code Execution	Critical	No	No	2
			CVE-2022-34708	Information Disclosure	Important	No	No	2
			CVE-2022-35753	Remote Code Execution	Critical	No	No	2
			CVE-2022-34707	Elevation of Privilege	Important	No	No	2
			CVE-2022-30133	Remote Code Execution	Critical	No	No	2
			CVE-2022-35767	Remote Code	Critical	No	No	2

				Execution				
			CVE-2022-34702	Remote Code Execution	Critical	No	No	2
			CVE-2022-35793	Elevation of Privilege	Important	No	No	1
			CVE-2022-35752	Remote Code Execution	Critical	No	No	2
5016616	高危	August 9, 2022 — KB5016616 (OS Builds 19042.1889, 19043.1889, and 19044.1889) for Windows Server, version 20H2, all editions ,Windows 10 Enterprise Multi-Session, version 20H2,Windows 10 Enterprise and Education, version 20H2,Windows 10	CVE-2022-34691	Elevation of Privilege	Critical	No	No	2
			CVE-2022-30197	Information Disclosure	Important	No	No	2
			CVE-2022-35762	Elevation of Privilege	Important	No	No	2
			CVE-2022-35744	Remote Code Execution	Critical	No	No	2
			CVE-2022-34714	Remote Code Execution	Critical	No	No	2
			CVE-2022-35750	Elevation of Privilege	Important	No	No	1
			CVE-2022-35754	Elevation of Privilege	Important	No	No	2
			CVE-2022-34706	Elevation of Privilege	Important	No	No	2
			CVE-2022-35758	Information Disclosure	Important	No	No	2
			CVE-2022-35748	Denial of Service	Important	No	No	1
			CVE-2022-34703	Elevation of Privilege	Important	No	No	1
			CVE-2022-35795	Elevation of Privilege	Important	No	No	2
			CVE-2022-34701	Denial of	Important	No	No	2

		IoT Enterprise, version 20H2,Windows 10 on Surface Hub,Windows 10, version 21H1, all editions,Windows 10, version 21H2, all editions		Service				
			CVE-2022-34709	Security Feature Bypass	Important	No	No	2
			CVE-2022-33670	Elevation of Privilege	Important	No	No	1
			CVE-2022-34710	Information Disclosure	Important	No	No	2
			CVE-2022-34699	Elevation of Privilege	Important	No	No	1
			CVE-2022-35764	Elevation of Privilege	Important	No	No	2
			CVE-2022-35768	Elevation of Privilege	Important	No	No	2
			CVE-2022-30144	Remote Code Execution	Important	No	No	2
			CVE-2022-35746	Elevation of Privilege	Important	No	No	2
			CVE-2022-34303	Security Feature Bypass	Important	No	No	1
			CVE-2022-35759	Denial of Service	Important	No	No	2
			CVE-2022-35755	Elevation of Privilege	Important	No	No	1
			CVE-2022-34713	Remote Code Execution	Important	Yes	Yes	0
			CVE-2022-35743	Remote Code Execution	Important	No	No	1
			CVE-2022-34690	Elevation of Privilege	Important	No	No	2
			CVE-2022-35747	Denial of Service	Important	No	No	2
			CVE-2022-35794	Remote Code	Critical	No	No	2

				Execution				
			CVE-2022-34705	Elevation of Privilege	Important	No	No	2
			CVE-2022-34301	Security Feature Bypass	Important	No	No	1
			CVE-2022-35749	Elevation of Privilege	Important	No	No	2
			CVE-2022-35765	Elevation of Privilege	Important	No	No	2
			CVE-2022-35751	Elevation of Privilege	Important	No	No	1
			CVE-2022-35760	Elevation of Privilege	Important	No	No	2
			CVE-2022-35769	Denial of Service	Important	No	No	2
			CVE-2022-34302	Security Feature Bypass	Important	No	No	1
			CVE-2022-35820	Elevation of Privilege	Important	No	No	1
			CVE-2022-35745	Remote Code Execution	Critical	No	No	2
			CVE-2022-34708	Information Disclosure	Important	No	No	2
			CVE-2022-30194	Remote Code Execution	Important	No	No	2
			CVE-2022-35761	Elevation of Privilege	Important	No	No	1
			CVE-2022-35766	Remote Code Execution	Critical	No	No	2
			CVE-2022-35753	Remote Code Execution	Critical	No	No	2
			CVE-2022-35756	Elevation	Important	No	No	1

				of Privilege				
			CVE-2022-34707	Elevation of Privilege	Important	No	No	2
			CVE-2022-30133	Remote Code Execution	Critical	No	No	2
			CVE-2022-34696	Remote Code Execution	Critical	No	No	2
			CVE-2022-35767	Remote Code Execution	Critical	No	No	2
			CVE-2022-35771	Elevation of Privilege	Important	No	No	2
			CVE-2022-34702	Remote Code Execution	Critical	No	No	2
			CVE-2022-35793	Elevation of Privilege	Important	No	No	1
			CVE-2022-35752	Remote Code Execution	Critical	No	No	2
			CVE-2022-35763	Elevation of Privilege	Important	No	No	2
			CVE-2022-34712	Information Disclosure	Important	No	No	2
			CVE-2022-35757	Elevation of Privilege	Important	No	No	2
			CVE-2022-35792	Elevation of Privilege	Important	No	No	2
			CVE-2022-35797	Security Feature Bypass	Important	No	No	2
			CVE-2022-34704	Information Disclosure	Important	No	No	2
5016622	高危	August 9, 2022 —	CVE-2022-34691	Elevation of Privilege	Critical	No	No	2

		KB5016622 (OS Build 14393.5291) for Windows 10, version 1607, all editions ,Windows Server 2016, all editions	CVE-2022-35762	Elevation of Privilege	Important	No	No	2
			CVE-2022-35744	Remote Code Execution	Critical	No	No	2
			CVE-2022-34714	Remote Code Execution	Critical	No	No	2
			CVE-2022-35750	Elevation of Privilege	Important	No	No	1
			CVE-2022-35754	Elevation of Privilege	Important	No	No	2
			CVE-2022-34706	Elevation of Privilege	Important	No	No	2
			CVE-2022-35758	Information Disclosure	Important	No	No	2
			CVE-2022-35748	Denial of Service	Important	No	No	1
			CVE-2022-34703	Elevation of Privilege	Important	No	No	1
			CVE-2022-35795	Elevation of Privilege	Important	No	No	2
			CVE-2022-34701	Denial of Service	Important	No	No	2
			CVE-2022-34709	Security Feature Bypass	Important	No	No	2
			CVE-2022-33670	Elevation of Privilege	Important	No	No	1
			CVE-2022-34710	Information Disclosure	Important	No	No	2
			CVE-2022-34699	Elevation of Privilege	Important	No	No	1
			CVE-2022-35764	Elevation	Important	No	No	2

				of Privilege				
			CVE-2022-35768	Elevation of Privilege	Important	No	No	2
			CVE-2022-30144	Remote Code Execution	Important	No	No	2
			CVE-2022-35746	Elevation of Privilege	Important	No	No	2
			CVE-2022-35759	Denial of Service	Important	No	No	2
			CVE-2022-35755	Elevation of Privilege	Important	No	No	1
			CVE-2022-34713	Remote Code Execution	Important	Yes	Yes	0
			CVE-2022-35743	Remote Code Execution	Important	No	No	1
			CVE-2022-34690	Elevation of Privilege	Important	No	No	2
			CVE-2022-35747	Denial of Service	Important	No	No	2
			CVE-2022-35749	Elevation of Privilege	Important	No	No	2
			CVE-2022-35765	Elevation of Privilege	Important	No	No	2
			CVE-2022-35751	Elevation of Privilege	Important	No	No	1
			CVE-2022-35760	Elevation of Privilege	Important	No	No	2
			CVE-2022-35769	Denial of Service	Important	No	No	2
			CVE-2022-30194	Remote Code Execution	Important	No	No	2
			CVE-2022-35745	Remote Code Execution	Critical	No	No	2

			CVE-2022-34708	Information Disclosure	Important	No	No	2
			CVE-2022-35761	Elevation of Privilege	Important	No	No	1
			CVE-2022-35753	Remote Code Execution	Critical	No	No	2
			CVE-2022-35756	Elevation of Privilege	Important	No	No	1
			CVE-2022-34707	Elevation of Privilege	Important	No	No	2
			CVE-2022-30133	Remote Code Execution	Critical	No	No	2
			CVE-2022-34696	Remote Code Execution	Critical	No	No	2
			CVE-2022-35767	Remote Code Execution	Critical	No	No	2
			CVE-2022-35771	Elevation of Privilege	Important	No	No	2
			CVE-2022-34702	Remote Code Execution	Critical	No	No	2
			CVE-2022-35793	Elevation of Privilege	Important	No	No	1
			CVE-2022-35752	Remote Code Execution	Critical	No	No	2
			CVE-2022-35763	Elevation of Privilege	Important	No	No	2
			CVE-2022-35792	Elevation of Privilege	Important	No	No	2
			CVE-2022-34704	Information Disclosure	Important	No	No	2
5016669	高危	August 9, 2022 —	CVE-2022-34691	Elevation of Privilege	Critical	No	No	2

		KB5016669 (Monthly Rollup) for Windows Server 2008 Datacenter ESU,Windows Server 2008 Standard ESU,Windows Server 2008 Enterprise ESU	CVE-2022-35744	Remote Code Execution	Critical	No	No	2
			CVE-2022-34714	Remote Code Execution	Critical	No	No	2
			CVE-2022-35750	Elevation of Privilege	Important	No	No	1
			CVE-2022-34706	Elevation of Privilege	Important	No	No	2
			CVE-2022-35758	Information Disclosure	Important	No	No	2
			CVE-2022-34701	Denial of Service	Important	No	No	2
			CVE-2022-35768	Elevation of Privilege	Important	No	No	2
			CVE-2022-35759	Denial of Service	Important	No	No	2
			CVE-2022-34690	Elevation of Privilege	Important	No	No	2
			CVE-2022-35747	Denial of Service	Important	No	No	2
			CVE-2022-35751	Elevation of Privilege	Important	No	No	1
			CVE-2022-35769	Denial of Service	Important	No	No	2
			CVE-2022-30194	Remote Code Execution	Important	No	No	2
			CVE-2022-35745	Remote Code Execution	Critical	No	No	2
			CVE-2022-34708	Information Disclosure	Important	No	No	2
			CVE-2022-35753	Remote Code Execution	Critical	No	No	2
			CVE-2022-34707	Elevation of Privilege	Important	No	No	2

			CVE-2022-30133	Remote Code Execution	Critical	No	No	2
			CVE-2022-35767	Remote Code Execution	Critical	No	No	2
			CVE-2022-34702	Remote Code Execution	Critical	No	No	2
			CVE-2022-35793	Elevation of Privilege	Important	No	No	1
			CVE-2022-35752	Remote Code Execution	Critical	No	No	2
5016681	高危	August 9, 2022 — KB5016681 (Monthly Rollup) 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-2022-34691	Elevation of Privilege	Critical	No	No	2
			CVE-2022-35744	Remote Code Execution	Critical	No	No	2
			CVE-2022-34714	Remote Code Execution	Critical	No	No	2
			CVE-2022-35750	Elevation of Privilege	Important	No	No	1
			CVE-2022-35754	Elevation of Privilege	Important	No	No	2
			CVE-2022-34706	Elevation of Privilege	Important	No	No	2
			CVE-2022-35758	Information Disclosure	Important	No	No	2
			CVE-2022-35748	Denial of Service	Important	No	No	1
			CVE-2022-35795	Elevation of Privilege	Important	No	No	2
			CVE-2022-34701	Denial of Service	Important	No	No	2
			CVE-2022-33670	Elevation of Privilege	Important	No	No	1
			CVE-2022-35768	Elevation of	Important	No	No	2

				Privilege				
			CVE-2022-30144	Remote Code Execution	Important	No	No	2
			CVE-2022-35746	Elevation of Privilege	Important	No	No	2
			CVE-2022-35759	Denial of Service	Important	No	No	2
			CVE-2022-35755	Elevation of Privilege	Important	No	No	1
			CVE-2022-34713	Remote Code Execution	Important	Yes	Yes	0
			CVE-2022-35743	Remote Code Execution	Important	No	No	1
			CVE-2022-34690	Elevation of Privilege	Important	No	No	2
			CVE-2022-35747	Denial of Service	Important	No	No	2
			CVE-2022-35749	Elevation of Privilege	Important	No	No	2
			CVE-2022-35751	Elevation of Privilege	Important	No	No	1
			CVE-2022-35760	Elevation of Privilege	Important	No	No	2
			CVE-2022-35769	Denial of Service	Important	No	No	2
			CVE-2022-35820	Elevation of Privilege	Important	No	No	1
			CVE-2022-35745	Remote Code Execution	Critical	No	No	2
			CVE-2022-34708	Information Disclosure	Important	No	No	2
			CVE-2022-30194	Remote Code Execution	Important	No	No	2
			CVE-2022-35753	Remote Code	Critical	No	No	2

				Execution				
			CVE-2022-35756	Elevation of Privilege	Important	No	No	1
			CVE-2022-34707	Elevation of Privilege	Important	No	No	2
			CVE-2022-30133	Remote Code Execution	Critical	No	No	2
			CVE-2022-34696	Remote Code Execution	Critical	No	No	2
			CVE-2022-35767	Remote Code Execution	Critical	No	No	2
			CVE-2022-34702	Remote Code Execution	Critical	No	No	2
			CVE-2022-35793	Elevation of Privilege	Important	No	No	1
			CVE-2022-35752	Remote Code Execution	Critical	No	No	2
5016683	高危	August 9, 2022 — KB5016683 (Security-only update) for Windows 8.1,Windows RT 8.1,Windows Server 2012 R2,Windows Embedded 8.1 Industry Enterpri	CVE-2022-34691	Elevation of Privilege	Critical	No	No	2
			CVE-2022-35744	Remote Code Execution	Critical	No	No	2
			CVE-2022-34714	Remote Code Execution	Critical	No	No	2
			CVE-2022-35750	Elevation of Privilege	Important	No	No	1
			CVE-2022-35754	Elevation of Privilege	Important	No	No	2
			CVE-2022-34706	Elevation of Privilege	Important	No	No	2
			CVE-2022-35758	Information Disclosure	Important	No	No	2
			CVE-2022-35748	Denial of Service	Important	No	No	1
			CVE-2022-35795	Elevation	Important	No	No	2

		se,Windows Embedded 8.1 Industry Pro		of Privilege				
			CVE-2022-34701	Denial of Service	Important	No	No	2
			CVE-2022-33670	Elevation of Privilege	Important	No	No	1
			CVE-2022-35768	Elevation of Privilege	Important	No	No	2
			CVE-2022-30144	Remote Code Execution	Important	No	No	2
			CVE-2022-35746	Elevation of Privilege	Important	No	No	2
			CVE-2022-35759	Denial of Service	Important	No	No	2
			CVE-2022-35755	Elevation of Privilege	Important	No	No	1
			CVE-2022-34713	Remote Code Execution	Important	Yes	Yes	0
			CVE-2022-35743	Remote Code Execution	Important	No	No	1
			CVE-2022-34690	Elevation of Privilege	Important	No	No	2
			CVE-2022-35747	Denial of Service	Important	No	No	2
			CVE-2022-35749	Elevation of Privilege	Important	No	No	2
			CVE-2022-35751	Elevation of Privilege	Important	No	No	1
			CVE-2022-35760	Elevation of Privilege	Important	No	No	2
			CVE-2022-35769	Denial of Service	Important	No	No	2
			CVE-2022-35820	Elevation of	Important	No	No	1

				Privilege				
			CVE-2022-35745	Remote Code Execution	Critical	No	No	2
			CVE-2022-34708	Information Disclosure	Important	No	No	2
			CVE-2022-30194	Remote Code Execution	Important	No	No	2
			CVE-2022-35753	Remote Code Execution	Critical	No	No	2
			CVE-2022-35756	Elevation of Privilege	Important	No	No	1
			CVE-2022-34707	Elevation of Privilege	Important	No	No	2
			CVE-2022-30133	Remote Code Execution	Critical	No	No	2
			CVE-2022-34696	Remote Code Execution	Critical	No	No	2
			CVE-2022-35767	Remote Code Execution	Critical	No	No	2
			CVE-2022-34702	Remote Code Execution	Critical	No	No	2
			CVE-2022-35793	Elevation of Privilege	Important	No	No	1
			CVE-2022-35752	Remote Code Execution	Critical	No	No	2
5016629	高危	August 9, 2022 — KB5016629 (OS Build 22000.856) for Windows 11	CVE-2022-34691	Elevation of Privilege	Critical	No	No	2
			CVE-2022-30197	Information Disclosure	Important	No	No	2
			CVE-2022-35744	Remote Code Execution	Critical	No	No	2
			CVE-2022-34714	Remote Code Execution	Critical	No	No	2
			CVE-2022-35750	Elevation of Privilege	Important	No	No	1

			CVE-2022-35754	Elevation of Privilege	Important	No	No	2
			CVE-2022-34706	Elevation of Privilege	Important	No	No	2
			CVE-2022-35758	Information Disclosure	Important	No	No	2
			CVE-2022-34703	Elevation of Privilege	Important	No	No	1
			CVE-2022-35795	Elevation of Privilege	Important	No	No	2
			CVE-2022-34701	Denial of Service	Important	No	No	2
			CVE-2022-34709	Security Feature Bypass	Important	No	No	2
			CVE-2022-33670	Elevation of Privilege	Important	No	No	1
			CVE-2022-34710	Information Disclosure	Important	No	No	2
			CVE-2022-34699	Elevation of Privilege	Important	No	No	1
			CVE-2022-35768	Elevation of Privilege	Important	No	No	2
			CVE-2022-30144	Remote Code Execution	Important	No	No	2
			CVE-2022-35746	Elevation of Privilege	Important	No	No	2
			CVE-2022-34303	Security Feature Bypass	Important	No	No	1
			CVE-2022-35759	Denial of Service	Important	No	No	2

			CVE-2022-35755	Elevation of Privilege	Important	No	No	1
			CVE-2022-34713	Remote Code Execution	Important	Yes	Yes	0
			CVE-2022-35743	Remote Code Execution	Important	No	No	1
			CVE-2022-34690	Elevation of Privilege	Important	No	No	2
			CVE-2022-35747	Denial of Service	Important	No	No	2
			CVE-2022-35794	Remote Code Execution	Critical	No	No	2
			CVE-2022-34705	Elevation of Privilege	Important	No	No	2
			CVE-2022-34301	Security Feature Bypass	Important	No	No	1
			CVE-2022-35749	Elevation of Privilege	Important	No	No	2
			CVE-2022-35751	Elevation of Privilege	Important	No	No	1
			CVE-2022-35760	Elevation of Privilege	Important	No	No	2
			CVE-2022-35769	Denial of Service	Important	No	No	2
			CVE-2022-34302	Security Feature Bypass	Important	No	No	1
			CVE-2022-35820	Elevation of Privilege	Important	No	No	1
			CVE-2022-35745	Remote Code Execution	Critical	No	No	2
			CVE-2022-34708	Information Disclosure	Important	No	No	2

			CVE-2022-30194	Remote Code Execution	Important	No	No	2
			CVE-2022-35761	Elevation of Privilege	Important	No	No	1
			CVE-2022-35766	Remote Code Execution	Critical	No	No	2
			CVE-2022-35753	Remote Code Execution	Critical	No	No	2
			CVE-2022-35756	Elevation of Privilege	Important	No	No	1
			CVE-2022-34707	Elevation of Privilege	Important	No	No	2
			CVE-2022-30133	Remote Code Execution	Critical	No	No	2
			CVE-2022-34696	Remote Code Execution	Critical	No	No	2
			CVE-2022-35767	Remote Code Execution	Critical	No	No	2
			CVE-2022-35771	Elevation of Privilege	Important	No	No	2
			CVE-2022-35804	Remote Code Execution	Critical	No	No	1
			CVE-2022-35793	Elevation of Privilege	Important	No	No	1
			CVE-2022-34702	Remote Code Execution	Critical	No	No	2
			CVE-2022-35752	Remote Code Execution	Critical	No	No	2
			CVE-2022-34712	Information Disclosure	Important	No	No	2
			CVE-2022-35757	Elevation of Privilege	Important	No	No	2
			CVE-2022-35797	Security Feature Bypass	Important	No	No	2

			CVE-2022-34704	Information Disclosure	Important	No	No	2
5016672	高危	August 9, 2022 — KB5016672 (Monthly Rollup) for Windows Server 2012,Windows Embedded 8 Standard	CVE-2022-34691	Elevation of Privilege	Critical	No	No	2
			CVE-2022-35744	Remote Code Execution	Critical	No	No	2
			CVE-2022-34714	Remote Code Execution	Critical	No	No	2
			CVE-2022-35750	Elevation of Privilege	Important	No	No	1
			CVE-2022-35754	Elevation of Privilege	Important	No	No	2
			CVE-2022-34706	Elevation of Privilege	Important	No	No	2
			CVE-2022-35758	Information Disclosure	Important	No	No	2
			CVE-2022-35748	Denial of Service	Important	No	No	1
			CVE-2022-35795	Elevation of Privilege	Important	No	No	2
			CVE-2022-34701	Denial of Service	Important	No	No	2
			CVE-2022-33670	Elevation of Privilege	Important	No	No	1
			CVE-2022-35768	Elevation of Privilege	Important	No	No	2
			CVE-2022-35746	Elevation of Privilege	Important	No	No	2
			CVE-2022-35759	Denial of Service	Important	No	No	2
			CVE-2022-34713	Remote Code Execution	Important	Yes	Yes	0

			CVE-2022-35743	Remote Code Execution	Important	No	No	1
			CVE-2022-34690	Elevation of Privilege	Important	No	No	2
			CVE-2022-35747	Denial of Service	Important	No	No	2
			CVE-2022-35749	Elevation of Privilege	Important	No	No	2
			CVE-2022-35751	Elevation of Privilege	Important	No	No	1
			CVE-2022-35760	Elevation of Privilege	Important	No	No	2
			CVE-2022-35769	Denial of Service	Important	No	No	2
			CVE-2022-35820	Elevation of Privilege	Important	No	No	1
			CVE-2022-35745	Remote Code Execution	Critical	No	No	2
			CVE-2022-34708	Information Disclosure	Important	No	No	2
			CVE-2022-30194	Remote Code Execution	Important	No	No	2
			CVE-2022-35753	Remote Code Execution	Critical	No	No	2
			CVE-2022-35756	Elevation of Privilege	Important	No	No	1
			CVE-2022-34707	Elevation of Privilege	Important	No	No	2
			CVE-2022-30133	Remote Code Execution	Critical	No	No	2
			CVE-2022-35767	Remote Code Execution	Critical	No	No	2
			CVE-2022-34702	Remote Code Execution	Critical	No	No	2

			CVE-2022-35793	Elevation of Privilege	Important	No	No	1
			CVE-2022-35752	Remote Code Execution	Critical	No	No	2
5016684	高危	August 9, 2022 — KB5016684 (Security-only update) for Windows Server 2012,Windows Embedded 8 Standard	CVE-2022-34691	Elevation of Privilege	Critical	No	No	2
			CVE-2022-35744	Remote Code Execution	Critical	No	No	2
			CVE-2022-34714	Remote Code Execution	Critical	No	No	2
			CVE-2022-35750	Elevation of Privilege	Important	No	No	1
			CVE-2022-35754	Elevation of Privilege	Important	No	No	2
			CVE-2022-34706	Elevation of Privilege	Important	No	No	2
			CVE-2022-35758	Information Disclosure	Important	No	No	2
			CVE-2022-35748	Denial of Service	Important	No	No	1
			CVE-2022-35795	Elevation of Privilege	Important	No	No	2
			CVE-2022-34701	Denial of Service	Important	No	No	2
			CVE-2022-33670	Elevation of Privilege	Important	No	No	1
			CVE-2022-35768	Elevation of Privilege	Important	No	No	2
			CVE-2022-35746	Elevation of Privilege	Important	No	No	2
			CVE-2022-35759	Denial of Service	Important	No	No	2

			CVE-2022-34713	Remote Code Execution	Important	Yes	Yes	0
			CVE-2022-35743	Remote Code Execution	Important	No	No	1
			CVE-2022-34690	Elevation of Privilege	Important	No	No	2
			CVE-2022-35747	Denial of Service	Important	No	No	2
			CVE-2022-35749	Elevation of Privilege	Important	No	No	2
			CVE-2022-35751	Elevation of Privilege	Important	No	No	1
			CVE-2022-35760	Elevation of Privilege	Important	No	No	2
			CVE-2022-35769	Denial of Service	Important	No	No	2
			CVE-2022-35820	Elevation of Privilege	Important	No	No	1
			CVE-2022-35745	Remote Code Execution	Critical	No	No	2
			CVE-2022-34708	Information Disclosure	Important	No	No	2
			CVE-2022-30194	Remote Code Execution	Important	No	No	2
			CVE-2022-35753	Remote Code Execution	Critical	No	No	2
			CVE-2022-35756	Elevation of Privilege	Important	No	No	1
			CVE-2022-34707	Elevation of Privilege	Important	No	No	2
			CVE-2022-30133	Remote Code Execution	Critical	No	No	2
			CVE-2022-35767	Remote Code Execution	Critical	No	No	2

			CVE-2022-34702	Remote Code Execution	Critical	No	No	2
			CVE-2022-35793	Elevation of Privilege	Important	No	No	1
			CVE-2022-35752	Remote Code Execution	Critical	No	No	2
5016676	高危	August 9, 2022 — KB5016676 (Monthly Rollup) for Windows 7 Enterprise ESU,Windows 7 Professional ESU,Windows 7 Ultimate ESU,Windows Server 2008 R2 Enterprise ESU,Windows Server 2008 R2 Standard ESU,Windows Server 2008 R2 Datacent	CVE-2022-34691	Elevation of Privilege	Critical	No	No	2
			CVE-2022-35744	Remote Code Execution	Critical	No	No	2
			CVE-2022-34714	Remote Code Execution	Critical	No	No	2
			CVE-2022-35750	Elevation of Privilege	Important	No	No	1
			CVE-2022-34706	Elevation of Privilege	Important	No	No	2
			CVE-2022-35758	Information Disclosure	Important	No	No	2
			CVE-2022-35795	Elevation of Privilege	Important	No	No	2
			CVE-2022-34701	Denial of Service	Important	No	No	2
			CVE-2022-35768	Elevation of Privilege	Important	No	No	2
			CVE-2022-35759	Denial of Service	Important	No	No	2
			CVE-2022-34713	Remote Code Execution	Important	Yes	Yes	0
			CVE-2022-35743	Remote Code Execution	Important	No	No	1
			CVE-2022-34690	Elevation of Privilege	Important	No	No	2
			CVE-2022-35747	Denial of Service	Important	No	No	2

		er ESU,Windows Embedded Standard 7 ESU,Windows Embedded POSReady 7 ESU	CVE-2022-35751	Elevation of Privilege	Important	No	No	1
			CVE-2022-35760	Elevation of Privilege	Important	No	No	2
			CVE-2022-35769	Denial of Service	Important	No	No	2
			CVE-2022-35820	Elevation of Privilege	Important	No	No	1
			CVE-2022-35745	Remote Code Execution	Critical	No	No	2
			CVE-2022-34708	Information Disclosure	Important	No	No	2
			CVE-2022-30194	Remote Code Execution	Important	No	No	2
			CVE-2022-35753	Remote Code Execution	Critical	No	No	2
			CVE-2022-35756	Elevation of Privilege	Important	No	No	1
			CVE-2022-34707	Elevation of Privilege	Important	No	No	2
			CVE-2022-30133	Remote Code Execution	Critical	No	No	2
			CVE-2022-35767	Remote Code Execution	Critical	No	No	2
			CVE-2022-34702	Remote Code Execution	Critical	No	No	2
			CVE-2022-35793	Elevation of Privilege	Important	No	No	1
			CVE-2022-35752	Remote Code Execution	Critical	No	No	2
5012170	高危	KB5012170: Security update for	CVE-2022-34303	Security Feature Bypass	Important	No	No	1
			CVE-2022-34301	Security Feature	Important	No	No	1

		Secure Boot DBX: August 9, 2022		Bypass				
			CVE-2022-35820	Elevation of Privilege	Important	No	No	1
			CVE-2022-34302	Security Feature Bypass	Important	No	No	1

本月微软发布的软件安全更新补丁共 9 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
5016618	高危	KB5016618: Cumulative security update for Internet Explorer: August 9, 2022	CVE-2022-34691	Elevation of Privilege	Critical	No	No	2
			CVE-2022-35744	Remote Code Execution	Critical	No	No	2
			CVE-2022-34714	Remote Code Execution	Critical	No	No	2
			CVE-2022-35750	Elevation of Privilege	Important	No	No	1
			CVE-2022-35754	Elevation of Privilege	Important	No	No	2
			CVE-2022-34706	Elevation of Privilege	Important	No	No	2
			CVE-2022-35758	Information Disclosure	Important	No	No	2
			CVE-2022-35795	Elevation of Privilege	Important	No	No	2
			CVE-2022-34701	Denial	Important	No	No	2

				of Service				
			CVE-2022-33670	Elevation of Privilege	Important	No	No	1
			CVE-2022-35768	Elevation of Privilege	Important	No	No	2
			CVE-2022-30144	Remote Code Execution	Important	No	No	2
			CVE-2022-35746	Elevation of Privilege	Important	No	No	2
			CVE-2022-35759	Denial of Service	Important	No	No	2
			CVE-2022-35755	Elevation of Privilege	Important	No	No	1
			CVE-2022-34713	Remote Code Execution	Important	Yes	Yes	0
			CVE-2022-35743	Remote Code Execution	Important	No	No	1
			CVE-2022-34690	Elevation of Privilege	Important	No	No	2
			CVE-2022-35747	Denial of Service	Important	No	No	2
			CVE-2022-35749	Elevation of	Important	No	No	2

				Privilege				
			CVE-2022-35760	Elevation of Privilege	Important	No	No	2
			CVE-2022-35769	Denial of Service	Important	No	No	2
			CVE-2022-35820	Elevation of Privilege	Important	No	No	1
			CVE-2022-35745	Remote Code Execution	Critical	No	No	2
			CVE-2022-34708	Information Disclosure	Important	No	No	2
			CVE-2022-30194	Remote Code Execution	Important	No	No	2
			CVE-2022-35753	Remote Code Execution	Critical	No	No	2
			CVE-2022-35756	Elevation of Privilege	Important	No	No	1
			CVE-2022-34707	Elevation of Privilege	Important	No	No	2
			CVE-2022-30133	Remote Code Execution	Critical	No	No	2
			CVE-2022-35767	Remote	Critical	No	No	2

				Code Execution				
			CVE-2022-34702	Remote Code Execution	Critical	No	No	2
			CVE-2022-35793	Elevation of Privilege	Important	No	No	1
			CVE-2022-35752	Remote Code Execution	Critical	No	No	2
4462148	高危	Description of the security update for Office 2016: August 9, 2022 (KB4462148)	CVE-2022-34717	Remote Code Execution	Important	No	No	2
4462142	高危	Description of the security update for Office 2013: August 9, 2022 (KB4462142)	CVE-2022-34717	Remote Code Execution	Important	No	No	2
5015321	高危	Description of the security update for Microsoft Exchange Server	CVE-2022-24477	Elevation of Privilege	Critical	No	No	1
			CVE-2022-30134	Information Disclosu	Important	Yes	No	3

		2013: August 9, 2022 (KB5015321)		re				
			CVE-2022-21980	Elevation of Privilege	Critical	No	No	1
			CVE-2022-21979	Information Disclosure	Important	No	No	2
			CVE-2022-24516	Elevation of Privilege	Critical	No	No	1
5002232	高危	Description of the security update for Excel 2016: August 9, 2022 (KB5002232)	CVE-2022-33631	Security Feature Bypass	Important	No	No	2
5001990	高危	Description of the security update for Outlook 2013: August 9, 2022 (KB5001990)	CVE-2022-35742	Denial of Service	Important	No	No	2
5002051	高危	Description of the security update for Outlook 2016: August 9, 2022 (KB5002051)	CVE-2022-35742	Denial of Service	Important	No	No	2

5002242	高危	Description of the security update for Excel 2013: August 9, 2022 (KB5002242)	CVE-2022-33631	Security Feature Bypass	Important	No	No	2
5015322	高危	Description of the security update for Microsoft Exchange Server 2019 and 2016: August 9, 2022 (KB5015322)	CVE-2022-34692	Information Disclosure	Important	No	No	2
			CVE-2022-24477	Elevation of Privilege	Critical	No	No	1
			CVE-2022-30134	Information Disclosure	Important	Yes	No	3
			CVE-2022-21980	Elevation of Privilege	Critical	No	No	1
			CVE-2022-21979	Information Disclosure	Important	No	No	2
			CVE-2022-24516	Elevation of Privilege	Critical	No	No	1

本月发布内容中还包括 2 个一般性更新补丁：

KBID	奇安信集团级别	详细信息
5002248	其他功能性补丁	Office 2016 更新程序
5002250	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