奇安信集团 2023 年 12 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 12 月 13 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 6

第 4 章 漏洞补丁详细列表 7

第 5 章 参考链接 20

文档信息

文档名称	奇安信集团 2023 年 12 月补丁库更新通告		
文档编号	Qi An Xin Group-MSPatch-2023-1201		
发布日期	2023-12-13	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:2023.12.13.1,V10版本:2023.12.13.1000)已发布，本次更新推送了16个微软安全补丁，修复了27个安全漏洞，其中3个微软官方评级为“严重(Critical)”，24个评级为“重要(Important)”，这些漏洞影响Windows、Internet Explorer、Office等产品。

第2章 重点关注补丁

本月有 12 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
5033427	CVE-2023-35641	Remote Code Execution	Critical	No	No	Exploitation More Likely
5033420						
5033422						
5033372						
5033375						
5033118						
5033371						
5033429						
5033379						
5033424						
5033433						
5033373						
5033369						
5033427	CVE-2023-35630	Remote Code Execution	Critical	No	No	Exploitation Less Likely
5033420						
5033422						
5033372						
5033375						
5033118						
5033371						
5033429						
5033379						
5033424						
5033433						
5033373						
5033369						
5033427	CVE-2023-35633	Elevation of Privilege	Important	No	No	Exploitation More Likely
5033420						

5033422						
5033429						
5033379						
5033424						
5033433						
5033427	CVE-2023-20588	Information Disclosure	Important	Yes	No	Exploitation Less Likely
5033420						
5033422						
5033372						
5033375						
5033118						
5033371						
5033429						
5033379						
5033424						
5033433						
5033373						
5033369						
5033427	CVE-2023-36005	Elevation of Privilege	Important	No	No	Exploitation More Likely
5033420						
5033422						
5033372						
5033375						
5033118						
5033371						
5033429						
5033379						
5033424						
5033433						
5033373						
5033369						
5033420	CVE-2023-35628	Remote Code Execution	Critical	No	No	Exploitation More Likely
5033372						
5033375						
5033118						
5033371						
5033429						
5033379						
5033424						
5033376						
5033433						

5033373						
5033369						
5033420	CVE-2023-35632	Elevation of Privilege	Important	No	No	Exploitation More Likely
5033372						
5033371						
5033429						
5033379						
5033424						
5033433						
5033373						
5033420	CVE-2023-36011	Elevation of Privilege	Important	No	No	Exploitation More Likely
5033372						
5033375						
5033118						
5033371						
5033429						
5033379						
5033373						
5033369						
5033372	CVE-2023-35644	Elevation of Privilege	Important	No	No	Exploitation More Likely
5033375						
5033118						
5033371						
5033369						
5033372	CVE-2023-36696	Elevation of Privilege	Important	No	No	Exploitation More Likely
5033375						
5033118						
5033371						
5033369						
5033375	CVE-2023-35631	Elevation of Privilege	Important	No	No	Exploitation More Likely
5033369						
5033375	CVE-2023-36391	Elevation of Privilege	Important	No	No	Exploitation More Likely

第3章 已知问题和特殊调整

本月暂无已知问题和特殊调整。

第4章 漏洞补丁详细列表

本月微软发布的系统安全更新补丁共 13 个，详细列表如下：

KBID	奇安信集团级别	补丁名称	CVE 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
5033427	高危	December 12, 2023—KB5033427 (Security-only update) - Microsoft Support for Windows Server 2008 Datacenter ESU,Windows Server 2008 Standard ESU,Windows Server 2008 Enterprise ESU	CVE-2023-35641	Remote Code Execution	Critical	No	No	1
			CVE-2023-35630	Remote Code Execution	Critical	No	No	2
			CVE-2023-35622	Spoofing	Important	No	No	2
			CVE-2023-35629	Remote Code Execution	Important	No	No	2
			CVE-2023-35633	Elevation of Privilege	Important	No	No	1
			CVE-2023-35639	Remote Code Execution	Important	No	No	2
			CVE-2023-35642	Denial of Service	Important	No	No	2
			CVE-2023-36004	Spoofing	Important	No	No	2
			CVE-2023-36006	Remote Code Execution	Important	No	No	2
			CVE-2023-36012	Information Disclosure	Important	No	No	2
			CVE-2023-20588	Information Disclosure	Important	Yes	No	2
			CVE-2023-36005	Elevation of Privilege	Important	No	No	1

5033420	高危	December 12, 2023—KB5033420 (Monthly Rollup) - Microsoft Support for Windows Server 2012 R2	CVE-2023-35641	Remote Code Execution	Critical	No	No	1
			CVE-2023-35630	Remote Code Execution	Critical	No	No	2
			CVE-2023-35622	Spoofing	Important	No	No	2
			CVE-2023-35628	Remote Code Execution	Critical	No	No	1
			CVE-2023-35633	Elevation of Privilege	Important	No	No	1
			CVE-2023-35629	Remote Code Execution	Important	No	No	2
			CVE-2023-35639	Remote Code Execution	Important	No	No	2
			CVE-2023-35642	Denial of Service	Important	No	No	2
			CVE-2023-36004	Spoofing	Important	No	No	2
			CVE-2023-36006	Remote Code Execution	Important	No	No	2
			CVE-2023-35632	Elevation of Privilege	Important	No	No	1
			CVE-2023-36011	Elevation of Privilege	Important	No	No	1
			CVE-2023-21740	Remote Code Execution	Important	No	No	2
			CVE-2023-36012	Information Disclosure	Important	No	No	2
			CVE-2023-35638	Denial of Service	Important	No	No	2
			CVE-2023-20588	Information Disclosure	Important	Yes	No	2
			CVE-2023-35643	Information Disclosure	Important	No	No	2
			CVE-2023-36005	Elevation of Privilege	Important	No	No	1
5033422	高危	December 12, 2023—KB5033422 (Monthly Rollup)	CVE-2023-35641	Remote Code Execution	Critical	No	No	1
			CVE-2023-35630	Remote Code Execution	Critical	No	No	2
			CVE-2023-35622	Spoofing	Important	No	No	2
			CVE-2023-35629	Remote Code Execution	Important	No	No	2

		- Microsoft Support for Windows Server 2008 Datacenter ESU,Windows Server 2008 Standard ESU,Windows Server 2008 Enterprise ESU	CVE-2023-35633	Elevation of Privilege	Important	No	No	1
			CVE-2023-35639	Remote Code Execution	Important	No	No	2
			CVE-2023-35642	Denial of Service	Important	No	No	2
			CVE-2023-36004	Spoofing	Important	No	No	2
			CVE-2023-36006	Remote Code Execution	Important	No	No	2
			CVE-2023-36012	Information Disclosure	Important	No	No	2
			CVE-2023-20588	Information Disclosure	Important	Yes	No	2
			CVE-2023-36005	Elevation of Privilege	Important	No	No	1
5033372	高危	December 12, 2023—KB5033372 (OS Builds 19044.3803 and 19045.3803) - Microsoft Support for Windows 10 Enterprise and Education, version	CVE-2023-35644	Elevation of Privilege	Important	No	No	1
			CVE-2023-35641	Remote Code Execution	Critical	No	No	1
			CVE-2023-35630	Remote Code Execution	Critical	No	No	2
			CVE-2023-36696	Elevation of Privilege	Important	No	No	1
			CVE-2023-35628	Remote Code Execution	Critical	No	No	1
			CVE-2023-35639	Remote Code Execution	Important	No	No	2
			CVE-2023-35642	Denial of Service	Important	No	No	2
			CVE-2023-36004	Spoofing	Important	No	No	2
			CVE-2023-36006	Remote Code Execution	Important	No	No	2
			CVE-2023-35632	Elevation of Privilege	Important	No	No	1
			CVE-2023-36003	Elevation of Privilege	Important	No	No	2

		21H2,Windows 10 IoT Enterprise, version 21H2,Windows 10 Enterprise Multi-Session, version 21H2,Windows 10, version 22H2, all editions	CVE-2023-36011	Elevation of Privilege	Important	No	No	1
			CVE-2023-21740	Remote Code Execution	Important	No	No	2
			CVE-2023-20588	Information Disclosure	Important	Yes	No	2
			CVE-2023-36005	Elevation of Privilege	Important	No	No	1
5033375	高危	December 12, 2023—KB5033375 (OS Builds 22621.2861 and 22631.2861) - Microsoft Support for Windows 11 version 22H2, all editions,Windows 11 version	CVE-2023-36696	Elevation of Privilege	Important	No	No	1
			CVE-2023-35641	Remote Code Execution	Critical	No	No	1
			CVE-2023-35630	Remote Code Execution	Critical	No	No	2
			CVE-2023-35644	Elevation of Privilege	Important	No	No	1
			CVE-2023-35628	Remote Code Execution	Critical	No	No	1
			CVE-2023-35634	Remote Code Execution	Important	No	No	2
			CVE-2023-35639	Remote Code Execution	Important	No	No	2
			CVE-2023-35642	Denial of Service	Important	No	No	2
			CVE-2023-36004	Spoofing	Important	No	No	2
			CVE-2023-36006	Remote Code Execution	Important	No	No	2
			CVE-2023-36003	Elevation of Privilege	Important	No	No	2
			CVE-2023-36011	Elevation of Privilege	Important	No	No	1

		23H2, all editions	CVE-2023-21740	Remote Code Execution	Important	No	No	2
			CVE-2023-35631	Elevation of Privilege	Important	No	No	1
			CVE-2023-36391	Elevation of Privilege	Important	No	No	1
			CVE-2023-35635	Denial of Service	Important	No	No	2
			CVE-2023-20588	Information Disclosure	Important	Yes	No	2
			CVE-2023-36005	Elevation of Privilege	Important	No	No	1
5033118	高危	December 12, 2023—KB5033118 (OS Build 20348.2159) - Microsoft Support for Windows Server 2022	CVE-2023-35644	Elevation of Privilege	Important	No	No	1
			CVE-2023-35641	Remote Code Execution	Critical	No	No	1
			CVE-2023-35630	Remote Code Execution	Critical	No	No	2
			CVE-2023-36696	Elevation of Privilege	Important	No	No	1
			CVE-2023-35622	Spoofing	Important	No	No	2
			CVE-2023-35628	Remote Code Execution	Critical	No	No	1
			CVE-2023-35639	Remote Code Execution	Important	No	No	2
			CVE-2023-35642	Denial of Service	Important	No	No	2
			CVE-2023-36004	Spoofing	Important	No	No	2
			CVE-2023-36006	Remote Code Execution	Important	No	No	2
			CVE-2023-36003	Elevation of Privilege	Important	No	No	2
			CVE-2023-36011	Elevation of Privilege	Important	No	No	1
			CVE-2023-21740	Remote Code Execution	Important	No	No	2
			CVE-2023-36012	Information Disclosure	Important	No	No	2
			CVE-2023-35638	Denial of Service	Important	No	No	2

			CVE-2023-20588	Information Disclosure	Important	Yes	No	2
			CVE-2023-35643	Information Disclosure	Important	No	No	2
			CVE-2023-36005	Elevation of Privilege	Important	No	No	1
5033371	高危	December 12, 2023—KB5033371 (OS Build 17763.5206) - Microsoft Support for Win 10 Ent LTSC 2019,Win 10 IoT Ent LTSC 2019,Windows 10 IoT Core 2019 LTSC,Windows Server 2019	CVE-2023-35639	Remote Code Execution	Important	No	No	2
			CVE-2023-36012	Information Disclosure	Important	No	No	2
			CVE-2023-35644	Elevation of Privilege	Important	No	No	1
			CVE-2023-35630	Remote Code Execution	Critical	No	No	2
			CVE-2023-35628	Remote Code Execution	Critical	No	No	1
			CVE-2023-20588	Information Disclosure	Important	Yes	No	2
			CVE-2023-36003	Elevation of Privilege	Important	No	No	2
			CVE-2023-36696	Elevation of Privilege	Important	No	No	1
			CVE-2023-35641	Remote Code Execution	Critical	No	No	1
			CVE-2023-36004	Spoofing	Important	No	No	2
			CVE-2023-36006	Remote Code Execution	Important	No	No	2
			CVE-2023-36011	Elevation of Privilege	Important	No	No	1
			CVE-2023-35643	Information Disclosure	Important	No	No	2
			CVE-2023-35622	Spoofing	Important	No	No	2
			CVE-2023-35642	Denial of Service	Important	No	No	2
			CVE-2023-35632	Elevation of Privilege	Important	No	No	1
			CVE-2023-21740	Remote Code Execution	Important	No	No	2
			CVE-2023-35638	Denial of Service	Important	No	No	2

			CVE-2023-36005	Elevation of Privilege	Important	No	No	1
5033429	高危	December 12, 2023—KB5033429 (Monthly Rollup) - Microsoft Support for Windows Server 2012	CVE-2023-35641	Remote Code Execution	Critical	No	No	1
			CVE-2023-35630	Remote Code Execution	Critical	No	No	2
			CVE-2023-35622	Spoofing	Important	No	No	2
			CVE-2023-35628	Remote Code Execution	Critical	No	No	1
			CVE-2023-35633	Elevation of Privilege	Important	No	No	1
			CVE-2023-35629	Remote Code Execution	Important	No	No	2
			CVE-2023-35639	Remote Code Execution	Important	No	No	2
			CVE-2023-35642	Denial of Service	Important	No	No	2
			CVE-2023-36004	Spoofing	Important	No	No	2
			CVE-2023-36006	Remote Code Execution	Important	No	No	2
			CVE-2023-35632	Elevation of Privilege	Important	No	No	1
			CVE-2023-36011	Elevation of Privilege	Important	No	No	1
			CVE-2023-21740	Remote Code Execution	Important	No	No	2
			CVE-2023-36012	Information Disclosure	Important	No	No	2
			CVE-2023-35638	Denial of Service	Important	No	No	2
			CVE-2023-20588	Information Disclosure	Important	Yes	No	2
			CVE-2023-35643	Information Disclosure	Important	No	No	2
			CVE-2023-36005	Elevation of Privilege	Important	No	No	1
5033379	高危	December 12, 2023—KB503337	CVE-2023-35641	Remote Code Execution	Critical	No	No	1
			CVE-2023-35630	Remote Code Execution	Critical	No	No	2

		9 (OS Build 10240.20345) - Microsoft Support for Windows 10	CVE-2023-35628	Remote Code Execution	Critical	No	No	1
			CVE-2023-35629	Remote Code Execution	Important	No	No	2
			CVE-2023-35633	Elevation of Privilege	Important	No	No	1
			CVE-2023-35639	Remote Code Execution	Important	No	No	2
			CVE-2023-35642	Denial of Service	Important	No	No	2
			CVE-2023-36004	Spoofing	Important	No	No	2
			CVE-2023-36006	Remote Code Execution	Important	No	No	2
			CVE-2023-35632	Elevation of Privilege	Important	No	No	1
			CVE-2023-36003	Elevation of Privilege	Important	No	No	2
			CVE-2023-36011	Elevation of Privilege	Important	No	No	1
			CVE-2023-21740	Remote Code Execution	Important	No	No	2
			CVE-2023-20588	Information Disclosure	Important	Yes	No	2
			CVE-2023-36005	Elevation of Privilege	Important	No	No	1
5033424	高危	December 12, 2023—KB5033424 (Security-only update) - Microsoft Support for Windows Server 2008 R2	CVE-2023-35641	Remote Code Execution	Critical	No	No	1
			CVE-2023-35630	Remote Code Execution	Critical	No	No	2
			CVE-2023-35622	Spoofing	Important	No	No	2
			CVE-2023-35628	Remote Code Execution	Critical	No	No	1
			CVE-2023-35633	Elevation of Privilege	Important	No	No	1
			CVE-2023-35629	Remote Code Execution	Important	No	No	2
			CVE-2023-35639	Remote Code Execution	Important	No	No	2
			CVE-2023-35642	Denial of Service	Important	No	No	2
			CVE-2023-36004	Spoofing	Important	No	No	2

		Enterprise ESU,Windows Server 2008 R2 Standard ESU,Windows Server 2008 R2 Datacenter ESU,Windows Embedded POSReady 7 ESU	CVE-2023-36006	Remote Code Execution	Important	No	No	2
			CVE-2023-35632	Elevation of Privilege	Important	No	No	1
			CVE-2023-21740	Remote Code Execution	Important	No	No	2
			CVE-2023-36012	Information Disclosure	Important	No	No	2
			CVE-2023-20588	Information Disclosure	Important	Yes	No	2
			CVE-2023-36005	Elevation of Privilege	Important	No	No	1
5033433	高危	December 12, 2023—KB5033433 (Monthly Rollup) - Microsoft Support for Windows Server 2008 R2 Enterprise ESU,Windows Server 2008 R2 Standard ESU,Windows	CVE-2023-35641	Remote Code Execution	Critical	No	No	1
			CVE-2023-35630	Remote Code Execution	Critical	No	No	2
			CVE-2023-35622	Spoofing	Important	No	No	2
			CVE-2023-35628	Remote Code Execution	Critical	No	No	1
			CVE-2023-35633	Elevation of Privilege	Important	No	No	1
			CVE-2023-35629	Remote Code Execution	Important	No	No	2
			CVE-2023-35639	Remote Code Execution	Important	No	No	2
			CVE-2023-35642	Denial of Service	Important	No	No	2
			CVE-2023-36004	Spoofing	Important	No	No	2
			CVE-2023-36006	Remote Code Execution	Important	No	No	2
			CVE-2023-35632	Elevation of Privilege	Important	No	No	1
			CVE-2023-21740	Remote Code Execution	Important	No	No	2
			CVE-2023-36012	Information Disclosure	Important	No	No	2

		Server 2008 R2 Datacenter ESU,Windows Embedded POSReady 7 ESU	CVE-2023-20588	Information Disclosure	Important	Yes	No	2
			CVE-2023-36005	Elevation of Privilege	Important	No	No	1
5033373	高危	December 12, 2023—KB5033373 (OS Build 14393.6529) - Microsoft Support for Windows 10, version 1607, all editions ,Windows Server 2016, all editions	CVE-2023-35641	Remote Code Execution	Critical	No	No	1
			CVE-2023-35630	Remote Code Execution	Critical	No	No	2
			CVE-2023-35622	Spoofing	Important	No	No	2
			CVE-2023-35628	Remote Code Execution	Critical	No	No	1
			CVE-2023-35639	Remote Code Execution	Important	No	No	2
			CVE-2023-35642	Denial of Service	Important	No	No	2
			CVE-2023-36004	Spoofing	Important	No	No	2
			CVE-2023-36006	Remote Code Execution	Important	No	No	2
			CVE-2023-35632	Elevation of Privilege	Important	No	No	1
			CVE-2023-36003	Elevation of Privilege	Important	No	No	2
			CVE-2023-36011	Elevation of Privilege	Important	No	No	1
			CVE-2023-21740	Remote Code Execution	Important	No	No	2
			CVE-2023-36012	Information Disclosure	Important	No	No	2
			CVE-2023-35638	Denial of Service	Important	No	No	2
			CVE-2023-20588	Information Disclosure	Important	Yes	No	2
			CVE-2023-35643	Information Disclosure	Important	No	No	2
			CVE-2023-36005	Elevation of Privilege	Important	No	No	1

5033369	高危	December 12, 2023—KB5033369 (OS Build 22000.2652) - Microsoft Support for Windows 11 version 21H2, all editions	CVE-2023-35644	Elevation of Privilege	Important	No	No	1
			CVE-2023-35641	Remote Code Execution	Critical	No	No	1
			CVE-2023-35630	Remote Code Execution	Critical	No	No	2
			CVE-2023-36696	Elevation of Privilege	Important	No	No	1
			CVE-2023-35628	Remote Code Execution	Critical	No	No	1
			CVE-2023-35634	Remote Code Execution	Important	No	No	2
			CVE-2023-35639	Remote Code Execution	Important	No	No	2
			CVE-2023-35642	Denial of Service	Important	No	No	2
			CVE-2023-36004	Spoofing	Important	No	No	2
			CVE-2023-36006	Remote Code Execution	Important	No	No	2
			CVE-2023-36003	Elevation of Privilege	Important	No	No	2
			CVE-2023-36011	Elevation of Privilege	Important	No	No	1
			CVE-2023-21740	Remote Code Execution	Important	No	No	2
			CVE-2023-35631	Elevation of Privilege	Important	No	No	1
			CVE-2023-20588	Information Disclosure	Important	Yes	No	2
			CVE-2023-36005	Elevation of Privilege	Important	No	No	1

本月微软发布的软件安全更新补丁共 3 个，详细列表如下：

KBID	奇安信集团级别	补丁名称	CVE 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
5002529	高危	Description of the security update for Outlook 2016: December 12, 2023 (KB5002529) - Microsoft Support	CVE-2023-35636	Information Disclosure	Important	No	No	2
5033376	高危	KB5033376: Cumulative security update for Internet Explorer: December 12, 2023 - Microsoft Support	CVE-2023-35628	Remote Code Execution	Critical	No	No	1
5002520	高危	Description of the security update for Word 2016: December 12, 2023 (KB5002520) - Microsoft Support	CVE-2023-36009	Information Disclosure	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