# 奇安信集团 2024 年 01 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**

**2024 年 01 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 . . . . . 6

第 4 章 漏洞补丁详细列表 . . . . . 7

第 5 章 参考链接 . . . . . 32

## 文档信息

| | | | |
|---|---|---|---|
| 文档名称 | 奇安信集团 2024 年 01 月补丁库更新通告 | | |
| 文档编号 | Qi An Xin Group-MSPatch-2024-0101 | | |
| 发布日期 | 2024-01-10 | 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:2024.01.10.1,V10版本:2024.01.10.1000)已发布，本次更新推送了28个微软安全补丁，修复了42个安全漏洞，其中8个微软官方评级为“严重(Critical)”，34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 9 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 |
|---|---|---|---|---|---|---|
| 5034184 | CVE-2024-20683 | Elevation of Privilege | Important | No | No | Exploitation More Likely |
| 5034169 | | | | | | |
| 5034167 | | | | | | |
| 5034119 | | | | | | |
| 5034129 | | | | | | |
| 5034121 | | | | | | |
| 5034173 | | | | | | |
| 5034122 | | | | | | |
| 5034127 | | | | | | |
| 5034134 | | | | | | |
| 5034171 | | | | | | |
| 5034123 | | | | | | |
| 5034176 | | | | | | |
| 5034184 | CVE-2024-21307 | Remote Code Execution | Important | No | No | Exploitation More Likely |
| 5034169 | | | | | | |
| 5034167 | | | | | | |
| 5034119 | | | | | | |
| 5034129 | | | | | | |
| 5034121 | | | | | | |
| 5034122 | | | | | | |
| 5034127 | | | | | | |
| 5034134 | | | | | | |
| 5034171 | | | | | | |
| 5034123 | | | | | | |
| 5034184 | CVE-2024-20653 | Elevation of Privilege | Important | No | No | Exploitation More Likely |
| 5034169 | | | | | | |
| 5034167 | | | | | | |
| 5034119 | | | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| 5034129 | | | | | | |
| 5034121 | | | | | | |
| 5034173 | | | | | | |
| 5034122 | | | | | | |
| 5034127 | | | | | | |
| 5034134 | | | | | | |
| 5034171 | | | | | | |
| 5034123 | | | | | | |
| 5034176 | | | | | | |
| 5034184 | CVE-2024-20674 | Security Feature Bypass | Critical | No | No | Exploitation More Likely |
| 5034169 | | | | | | |
| 5034167 | | | | | | |
| 5034119 | | | | | | |
| 5034129 | | | | | | |
| 5034121 | | | | | | |
| 5034173 | | | | | | |
| 5034122 | | | | | | |
| 5034127 | | | | | | |
| 5034134 | | | | | | |
| 5034171 | | | | | | |
| 5034123 | | | | | | |
| 5034176 | | | | | | |
| 5034184 | CVE-2024-20652 | Security Feature Bypass | Important | No | No | Exploitation More Likely |
| 5034169 | | | | | | |
| 5034167 | | | | | | |
| 5034119 | | | | | | |
| 5034129 | | | | | | |
| 5034121 | | | | | | |
| 5034122 | | | | | | |
| 5034127 | | | | | | |
| 5034120 | | | | | | |
| 5034134 | | | | | | |
| 5034171 | | | | | | |
| 5034123 | | | | | | |
| 5034129 | CVE-2024-20698 | Elevation of Privilege | Important | No | No | Exploitation More Likely |
| 5034121 | | | | | | |
| 5034122 | | | | | | |
| 5034127 | | | | | | |
| 5034123 | | | | | | |
| 5034129 | CVE-2024-20700 | Remote Code Execution | Critical | No | No | Exploitation Less Likely |
| 5034121 | | | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| 5034122 | | | | | | |
| 5034127 | | | | | | |
| 5034123 | | | | | | |
| 5034129 | CVE-2024-21310 | Elevation of Privilege | Important | No | No | Exploitation More Likely |
| 5034121 | | | | | | |
| 5034122 | | | | | | |
| 5034127 | | | | | | |
| 5034123 | | | | | | |
| 5002541 | CVE-2024-21318 | Remote Code Execution | 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 |
|---|---|---|---|---|---|---|---|---|
| 5034184 | 高危 | January 9, 2024—KB5034184 (Monthly Rollup) - Microsoft Support for Windows Server 2012 ESU | CVE-2024-20655 | Remote Code Execution | Important | No | No | 2 |
| | | | CVE-2024-20658 | Elevation of Privilege | Important | No | No | 2 |
| | | | CVE-2024-20683 | Elevation of Privilege | Important | No | No | 1 |
| | | | CVE-2024-20661 | Denial of Service | Important | No | No | 2 |
| | | | CVE-2024-20657 | Elevation of Privilege | Important | No | No | 2 |
| | | | CVE-2024-21307 | Remote Code Execution | Important | No | No | 1 |
| | | | CVE-2024-20653 | Elevation of Privilege | Important | No | No | 1 |
| | | | CVE-2024-20664 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-20674 | Security Feature Bypass | Critical | No | No | 1 |
| | | | CVE-2024-21314 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-20692 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-20652 | Security Feature Bypass | Important | No | No | 1 |
| | | | CVE-2024-21313 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-21311 | Information Disclosure | Important | No | No | 2 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | CVE-2024-20691 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-20663 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-20662 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-21320 | Spoofing | Important | No | No | 2 |
| | | | CVE-2024-20660 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-20654 | Remote Code Execution | Important | No | No | 2 |
| | | | CVE-2024-20682 | Remote Code Execution | Important | No | No | 2 |
| | | | CVE-2024-20680 | Information Disclosure | Important | No | No | 2 |
| 5034169 | 高危 | January 9, 2024—KB5034169 (Monthly Rollup) - Microsoft Support for Windows Server 2008 R2 Enterprise ESU,Windows Server 2008 R2 Standard ESU,Windows Server 2008 R2 | CVE-2024-20655 | Remote Code Execution | Important | No | No | 2 |
| | | | CVE-2024-20683 | Elevation of Privilege | Important | No | No | 1 |
| | | | CVE-2024-20661 | Denial of Service | Important | No | No | 2 |
| | | | CVE-2024-20657 | Elevation of Privilege | Important | No | No | 2 |
| | | | CVE-2024-21307 | Remote Code Execution | Important | No | No | 1 |
| | | | CVE-2024-20653 | Elevation of Privilege | Important | No | No | 1 |
| | | | CVE-2024-20664 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-20674 | Security Feature Bypass | Critical | No | No | 1 |
| | | | CVE-2024-21314 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-20692 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-20652 | Security Feature Bypass | Important | No | No | 1 |
| | | | CVE-2024-21313 | Information Disclosure | Important | No | No | 2 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | Datacenter ESU,Windows Embedded POSReady 7 ESU | CVE-2024-21311 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-20691 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-20663 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-20662 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-20660 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-20654 | Remote Code Execution | Important | No | No | 2 |
| | | | CVE-2024-20680 | Information Disclosure | Important | No | No | 2 |
| 5034167 | 高危 | January 9, 2024—KB5034167 (Security-only update) - Microsoft Support for Windows Server 2008 R2 Enterprise ESU,Windows Server 2008 R2 Standard ESU,Windows Server | CVE-2024-20655 | Remote Code Execution | Important | No | No | 2 |
| | | | CVE-2024-20683 | Elevation of Privilege | Important | No | No | 1 |
| | | | CVE-2024-20661 | Denial of Service | Important | No | No | 2 |
| | | | CVE-2024-20657 | Elevation of Privilege | Important | No | No | 2 |
| | | | CVE-2024-21307 | Remote Code Execution | Important | No | No | 1 |
| | | | CVE-2024-20653 | Elevation of Privilege | Important | No | No | 1 |
| | | | CVE-2024-20664 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-20674 | Security Feature Bypass | Critical | No | No | 1 |
| | | | CVE-2024-21314 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-20692 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-20652 | Security Feature Bypass | Important | No | No | 1 |
| | | | CVE-2024-21313 | Information Disclosure | Important | No | No | 2 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | 2008 R2 Datacenter ESU,Windows Embedded POSReady 7 ESU | CVE-2024-21311 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-20691 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-20663 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-20662 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-20660 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-20654 | Remote Code Execution | Important | No | No | 2 |
| | | | CVE-2024-20680 | Information Disclosure | Important | No | No | 2 |
| 5034119 | 高危 | January 9, 2024—KB5034119 (OS Build 14393.6614) - Microsoft Support for Windows 10, version 1607, all editions ,Windows Server 2016, all editions | CVE-2024-20655 | Remote Code Execution | Important | No | No | 2 |
| | | | CVE-2024-20658 | Elevation of Privilege | Important | No | No | 2 |
| | | | CVE-2024-21312 | Denial of Service | Important | No | No | 2 |
| | | | CVE-2024-20683 | Elevation of Privilege | Important | No | No | 1 |
| | | | CVE-2024-20661 | Denial of Service | Important | No | No | 2 |
| | | | CVE-2024-20657 | Elevation of Privilege | Important | No | No | 2 |
| | | | CVE-2024-21307 | Remote Code Execution | Important | No | No | 1 |
| | | | CVE-2024-0057 | Security Feature Bypass | Important | No | No | 2 |
| | | | CVE-2024-20653 | Elevation of Privilege | Important | No | No | 1 |
| | | | CVE-2024-20664 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-20674 | Security Feature Bypass | Critical | No | No | 1 |
| | | | CVE-2024-20666 | Security Feature Bypass | Important | No | No | 2 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | CVE-2024-21314 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-20692 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-20652 | Security Feature Bypass | Important | No | No | 1 |
| | | | CVE-2024-0056 | Security Feature Bypass | Important | No | No | 2 |
| | | | CVE-2024-21313 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-21311 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-20691 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-20663 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-20694 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-20662 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-20687 | Denial of Service | Important | No | No | 2 |
| | | | CVE-2024-21320 | Spoofing | Important | No | No | 2 |
| | | | CVE-2024-20660 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-21316 | Security Feature Bypass | Important | No | No | 2 |
| | | | CVE-2024-20654 | Remote Code Execution | Important | No | No | 2 |
| | | | CVE-2024-20682 | Remote Code Execution | Important | No | No | 2 |
| | | | CVE-2024-20680 | Information Disclosure | Important | No | No | 2 |
| 5034129 | 高危 | January 9, 2024—KB503412 | CVE-2024-20655 | Remote Code Execution | Important | No | No | 2 |
| | | | CVE-2024-20658 | Elevation of Privilege | Important | No | No | 2 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | 9 (OS Build 20348.2227) - Microsoft Support for Windows Server 2022 | CVE-2024-20681 | Elevation of Privilege | Important | No | No | 2 |
| | | | CVE-2024-20683 | Elevation of Privilege | Important | No | No | 1 |
| | | | CVE-2024-20661 | Denial of Service | Important | No | No | 2 |
| | | | CVE-2024-21305 | Security Feature Bypass | Important | No | No | 2 |
| | | | CVE-2024-20657 | Elevation of Privilege | Important | No | No | 2 |
| | | | CVE-2024-21307 | Remote Code Execution | Important | No | No | 1 |
| | | | CVE-2024-20698 | Elevation of Privilege | Important | No | No | 1 |
| | | | CVE-2024-21309 | Elevation of Privilege | Important | No | No | 2 |
| | | | CVE-2024-20696 | Remote Code Execution | Important | No | No | 2 |
| | | | CVE-2024-20653 | Elevation of Privilege | Important | No | No | 1 |
| | | | CVE-2024-20664 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-20674 | Security Feature Bypass | Critical | No | No | 1 |
| | | | CVE-2024-20666 | Security Feature Bypass | Important | No | No | 2 |
| | | | CVE-2024-21314 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-21306 | Spoofing | Important | No | No | 2 |
| | | | CVE-2024-20692 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-20652 | Security Feature Bypass | Important | No | No | 1 |
| | | | CVE-2024-21313 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-20700 | Remote Code Execution | Critical | No | No | 2 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | CVE-2024-21311 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-20691 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-20663 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2022-35737 | | | No | No | 2 |
| | | | CVE-2024-20694 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-20662 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-20687 | Denial of Service | Important | No | No | 2 |
| | | | CVE-2024-21320 | Spoofing | Important | No | No | 2 |
| | | | CVE-2024-20699 | Denial of Service | Important | No | No | 2 |
| | | | CVE-2024-20660 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-21316 | Security Feature Bypass | Important | No | No | 2 |
| | | | CVE-2024-20654 | Remote Code Execution | Important | No | No | 2 |
| | | | CVE-2024-20682 | Remote Code Execution | Important | No | No | 2 |
| | | | CVE-2024-21310 | Elevation of Privilege | Important | No | No | 1 |
| | | | CVE-2024-20680 | Information Disclosure | Important | No | No | 2 |
| 5034121 | 高危 | January 9, 2024—KB5034121 (OS Build 22000.2713) - Microsoft Support | CVE-2024-20658 | Elevation of Privilege | Important | No | No | 2 |
| | | | CVE-2024-20681 | Elevation of Privilege | Important | No | No | 2 |
| | | | CVE-2024-20683 | Elevation of Privilege | Important | No | No | 1 |
| | | | CVE-2024-20661 | Denial of Service | Important | No | No | 2 |
| | | | CVE-2024-21305 | Security Feature Bypass | Important | No | No | 2 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | for Windows 11 version 21H2, all editions | CVE-2024-20657 | Elevation of Privilege | Important | No | No | 2 |
| | | | CVE-2024-21307 | Remote Code Execution | Important | No | No | 1 |
| | | | CVE-2024-20698 | Elevation of Privilege | Important | No | No | 1 |
| | | | CVE-2024-21309 | Elevation of Privilege | Important | No | No | 2 |
| | | | CVE-2024-20696 | Remote Code Execution | Important | No | No | 2 |
| | | | CVE-2024-20690 | Spoofing | Important | No | No | 2 |
| | | | CVE-2024-20653 | Elevation of Privilege | Important | No | No | 1 |
| | | | CVE-2024-20664 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-20674 | Security Feature Bypass | Critical | No | No | 1 |
| | | | CVE-2024-20666 | Security Feature Bypass | Important | No | No | 2 |
| | | | CVE-2024-21314 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-21306 | Spoofing | Important | No | No | 2 |
| | | | CVE-2024-20692 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-20652 | Security Feature Bypass | Important | No | No | 1 |
| | | | CVE-2024-21313 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-20700 | Remote Code Execution | Critical | No | No | 2 |
| | | | CVE-2024-21311 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-20691 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-20663 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-20694 | Information Disclosure | Important | No | No | 2 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | CVE-2024-20687 | Denial of Service | Important | No | No | 2 |
| | | | CVE-2024-21320 | Spoofing | Important | No | No | 2 |
| | | | CVE-2024-20699 | Denial of Service | Important | No | No | 2 |
| | | | CVE-2024-20660 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-21316 | Security Feature Bypass | Important | No | No | 2 |
| | | | CVE-2024-20654 | Remote Code Execution | Important | No | No | 2 |
| | | | CVE-2024-20682 | Remote Code Execution | Important | No | No | 2 |
| | | | CVE-2024-21310 | Elevation of Privilege | Important | No | No | 1 |
| | | | CVE-2024-20680 | Information Disclosure | Important | No | No | 2 |
| 5034173 | 高危 | January 9, 2024—KB5034173 (Monthly Rollup) - Microsoft Support for Windows Server 2008 Datacenter ESU,Windows Server 2008 Standard ESU,Wind | CVE-2024-21311 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-20663 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-20655 | Remote Code Execution | Important | No | No | 2 |
| | | | CVE-2024-20662 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-20683 | Elevation of Privilege | Important | No | No | 1 |
| | | | CVE-2024-20661 | Denial of Service | Important | No | No | 2 |
| | | | CVE-2024-20692 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-20653 | Elevation of Privilege | Important | No | No | 1 |
| | | | CVE-2024-20664 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-20674 | Security Feature Bypass | Critical | No | No | 1 |
| | | | CVE-2024-20660 | Information Disclosure | Important | No | No | 2 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | ows Server 2008 Enterprise ESU | CVE-2024-20657 | Elevation of Privilege | Important | No | No | 2 |
| | | | CVE-2024-21313 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-20654 | Remote Code Execution | Important | No | No | 2 |
| | | | CVE-2024-21314 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-20680 | Information Disclosure | Important | No | No | 2 |
| 5034122 | 高危 | January 9, 2024—KB5034122 (OS Builds 19044.3930 and 19045.3930) - Microsoft Support for Windows 10 Enterprise and Education, version 21H2, Windows 10 IoT Enterprise, version 21H2, Windows 10 Enterpri | CVE-2024-20658 | Elevation of Privilege | Important | No | No | 2 |
| | | | CVE-2024-20681 | Elevation of Privilege | Important | No | No | 2 |
| | | | CVE-2024-20683 | Elevation of Privilege | Important | No | No | 1 |
| | | | CVE-2024-20661 | Denial of Service | Important | No | No | 2 |
| | | | CVE-2024-21305 | Security Feature Bypass | Important | No | No | 2 |
| | | | CVE-2024-20657 | Elevation of Privilege | Important | No | No | 2 |
| | | | CVE-2024-21307 | Remote Code Execution | Important | No | No | 1 |
| | | | CVE-2024-20698 | Elevation of Privilege | Important | No | No | 1 |
| | | | CVE-2024-20696 | Remote Code Execution | Important | No | No | 2 |
| | | | CVE-2024-20690 | Spoofing | Important | No | No | 2 |
| | | | CVE-2024-20653 | Elevation of Privilege | Important | No | No | 1 |
| | | | CVE-2024-20664 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-20674 | Security Feature Bypass | Critical | No | No | 1 |
| | | | CVE-2024-20666 | Security Feature Bypass | Important | No | No | 2 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | se Multi-Session, version 21H2,Windows 10, version 22H2, all editions | CVE-2024-21314 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-21306 | Spoofing | Important | No | No | 2 |
| | | | CVE-2024-20692 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-20652 | Security Feature Bypass | Important | No | No | 1 |
| | | | CVE-2024-21313 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-20700 | Remote Code Execution | Critical | No | No | 2 |
| | | | CVE-2024-21311 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-20691 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-20663 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2022-35737 | | | No | No | 2 |
| | | | CVE-2024-20694 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-20687 | Denial of Service | Important | No | No | 2 |
| | | | CVE-2024-21320 | Spoofing | Important | No | No | 2 |
| | | | CVE-2024-20699 | Denial of Service | Important | No | No | 2 |
| | | | CVE-2024-20660 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-21316 | Security Feature Bypass | Important | No | No | 2 |
| | | | CVE-2024-20654 | Remote Code Execution | Important | No | No | 2 |
| | | | CVE-2024-20682 | Remote Code Execution | Important | No | No | 2 |
| | | | CVE-2024-21310 | Elevation of Privilege | Important | No | No | 1 |
| | | | CVE-2024-20680 | Information Disclosure | Important | No | No | 2 |
| 5034127 | 高危 | January 9, | CVE-2024-20655 | Remote Code Execution | Important | No | No | 2 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | 2024—KB5034127 (OS Build 17763.5329) - Microsoft Support for Win 10 Ent LTSC 2019,Win 10 IoT Ent LTSC 2019,Windows 10 IoT Core 2019 LTSC,Windows Server 2019 | CVE-2024-20658 | Elevation of Privilege | Important | No | No | 2 |
| | | | CVE-2024-20683 | Elevation of Privilege | Important | No | No | 1 |
| | | | CVE-2024-20661 | Denial of Service | Important | No | No | 2 |
| | | | CVE-2024-21305 | Security Feature Bypass | Important | No | No | 2 |
| | | | CVE-2024-20657 | Elevation of Privilege | Important | No | No | 2 |
| | | | CVE-2024-21307 | Remote Code Execution | Important | No | No | 1 |
| | | | CVE-2024-20698 | Elevation of Privilege | Important | No | No | 1 |
| | | | CVE-2024-20696 | Remote Code Execution | Important | No | No | 2 |
| | | | CVE-2024-20690 | Spoofing | Important | No | No | 2 |
| | | | CVE-2024-20653 | Elevation of Privilege | Important | No | No | 1 |
| | | | CVE-2024-20664 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-20674 | Security Feature Bypass | Critical | No | No | 1 |
| | | | CVE-2024-20666 | Security Feature Bypass | Important | No | No | 2 |
| | | | CVE-2024-21314 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-20692 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-20652 | Security Feature Bypass | Important | No | No | 1 |
| | | | CVE-2024-21313 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-20700 | Remote Code Execution | Critical | No | No | 2 |
| | | | CVE-2024-21311 | Information Disclosure | Important | No | No | 2 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | CVE-2024-20691 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-20663 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2022-35737 | | | No | No | 2 |
| | | | CVE-2024-20694 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-20662 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-20687 | Denial of Service | Important | No | No | 2 |
| | | | CVE-2024-21320 | Spoofing | Important | No | No | 2 |
| | | | CVE-2024-20699 | Denial of Service | Important | No | No | 2 |
| | | | CVE-2024-20660 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-21316 | Security Feature Bypass | Important | No | No | 2 |
| | | | CVE-2024-20654 | Remote Code Execution | Important | No | No | 2 |
| | | | CVE-2024-20682 | Remote Code Execution | Important | No | No | 2 |
| | | | CVE-2024-21310 | Elevation of Privilege | Important | No | No | 1 |
| | | | CVE-2024-20680 | Information Disclosure | Important | No | No | 2 |
| 5034134 | 高危 | January 9, 2024—KB5034134 (OS Build 10240.20402) - Microsoft Support for Windows 10 | CVE-2024-20658 | Elevation of Privilege | Important | No | No | 2 |
| | | | CVE-2024-20683 | Elevation of Privilege | Important | No | No | 1 |
| | | | CVE-2024-20661 | Denial of Service | Important | No | No | 2 |
| | | | CVE-2024-20657 | Elevation of Privilege | Important | No | No | 2 |
| | | | CVE-2024-21307 | Remote Code Execution | Important | No | No | 1 |
| | | | CVE-2024-20653 | Elevation of Privilege | Important | No | No | 1 |
| | | | CVE-2024-20664 | Information Disclosure | Important | No | No | 2 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | CVE-2024-20674 | Security Feature Bypass | Critical | No | No | 1 |
| | | | CVE-2024-20666 | Security Feature Bypass | Important | No | No | 2 |
| | | | CVE-2024-21314 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-20692 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-20652 | Security Feature Bypass | Important | No | No | 1 |
| | | | CVE-2024-21313 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-21311 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-20691 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-20663 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-20687 | Denial of Service | Important | No | No | 2 |
| | | | CVE-2024-21320 | Spoofing | Important | No | No | 2 |
| | | | CVE-2024-20660 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-20654 | Remote Code Execution | Important | No | No | 2 |
| | | | CVE-2024-20682 | Remote Code Execution | Important | No | No | 2 |
| | | | CVE-2024-20680 | Information Disclosure | Important | No | No | 2 |
| 5034171 | 高危 | January 9, 2024—KB5034171 (Monthly Rollup) - | CVE-2024-20655 | Remote Code Execution | Important | No | No | 2 |
| | | | CVE-2024-20658 | Elevation of Privilege | Important | No | No | 2 |
| | | | CVE-2024-20683 | Elevation of Privilege | Important | No | No | 1 |
| | | | CVE-2024-20661 | Denial of Service | Important | No | No | 2 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | Microsoft Support for Windows Server 2012 R2 ESU | CVE-2024-20657 | Elevation of Privilege | Important | No | No | 2 |
| | | | CVE-2024-21307 | Remote Code Execution | Important | No | No | 1 |
| | | | CVE-2024-20653 | Elevation of Privilege | Important | No | No | 1 |
| | | | CVE-2024-20664 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-20674 | Security Feature Bypass | Critical | No | No | 1 |
| | | | CVE-2024-21314 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-20692 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-20652 | Security Feature Bypass | Important | No | No | 1 |
| | | | CVE-2024-21313 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-21311 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-20691 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-20663 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-20662 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-21320 | Spoofing | Important | No | No | 2 |
| | | | CVE-2024-20660 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-20654 | Remote Code Execution | Important | No | No | 2 |
| | | | CVE-2024-20682 | Remote Code Execution | Important | No | No | 2 |
| | | | CVE-2024-20680 | Information Disclosure | Important | No | No | 2 |
| 5034123 | 高危 | January 9, 2024—KB503412 | CVE-2024-20658 | Elevation of Privilege | Important | No | No | 2 |
| | | | CVE-2024-20681 | Elevation of Privilege | Important | No | No | 2 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | 3 (OS Builds 22621.3007 and 22631.3007) - Microsoft Support for Windows 11 version 22H2, all editions,Windows 11 version 23H2, all editions | CVE-2024-20683 | Elevation of Privilege | Important | No | No | 1 |
| | | | CVE-2024-20661 | Denial of Service | Important | No | No | 2 |
| | | | CVE-2024-21305 | Security Feature Bypass | Important | No | No | 2 |
| | | | CVE-2024-20657 | Elevation of Privilege | Important | No | No | 2 |
| | | | CVE-2024-21307 | Remote Code Execution | Important | No | No | 1 |
| | | | CVE-2024-20698 | Elevation of Privilege | Important | No | No | 1 |
| | | | CVE-2024-21309 | Elevation of Privilege | Important | No | No | 2 |
| | | | CVE-2024-20697 | Remote Code Execution | Important | No | No | 2 |
| | | | CVE-2024-20696 | Remote Code Execution | Important | No | No | 2 |
| | | | CVE-2024-20690 | Spoofing | Important | No | No | 2 |
| | | | CVE-2024-20653 | Elevation of Privilege | Important | No | No | 1 |
| | | | CVE-2024-20664 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-20674 | Security Feature Bypass | Critical | No | No | 1 |
| | | | CVE-2024-20666 | Security Feature Bypass | Important | No | No | 2 |
| | | | CVE-2024-21314 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-21306 | Spoofing | Important | No | No | 2 |
| | | | CVE-2024-20692 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-20652 | Security Feature Bypass | Important | No | No | 1 |
| | | | CVE-2024-21313 | Information Disclosure | Important | No | No | 2 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | CVE-2024-20700 | Remote Code Execution | Critical | No | No | 2 |
| | | | CVE-2024-21311 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-20691 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-20663 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-20694 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-20687 | Denial of Service | Important | No | No | 2 |
| | | | CVE-2024-21320 | Spoofing | Important | No | No | 2 |
| | | | CVE-2024-20699 | Denial of Service | Important | No | No | 2 |
| | | | CVE-2024-20660 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-21316 | Security Feature Bypass | Important | No | No | 2 |
| | | | CVE-2024-20654 | Remote Code Execution | Important | No | No | 2 |
| | | | CVE-2024-20682 | Remote Code Execution | Important | No | No | 2 |
| | | | CVE-2024-21310 | Elevation of Privilege | Important | No | No | 1 |
| | | | CVE-2024-20680 | Information Disclosure | Important | No | No | 2 |
| 5034176 | 高危 | January 9, 2024—KB5034176 (Security-only update) - Microsoft Support | CVE-2024-21311 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-20663 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-20655 | Remote Code Execution | Important | No | No | 2 |
| | | | CVE-2024-20662 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-20683 | Elevation of Privilege | Important | No | No | 1 |
| | | | CVE-2024-20661 | Denial of Service | Important | No | No | 2 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | for Windows Server 2008 Datacenter ESU,Windows Server 2008 Standard ESU,Windows Server 2008 Enterprise ESU | CVE-2024-20692 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-20653 | Elevation of Privilege | Important | No | No | 1 |
| | | | CVE-2024-20664 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-20674 | Security Feature Bypass | Critical | No | No | 1 |
| | | | CVE-2024-20660 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-20657 | Elevation of Privilege | Important | No | No | 2 |
| | | | CVE-2024-21313 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-20654 | Remote Code Execution | Important | No | No | 2 |
| | | | CVE-2024-21314 | Information Disclosure | Important | No | No | 2 |
| | | | CVE-2024-20680 | Information Disclosure | Important | No | No | 2 |

本月微软发布的软件安全更新补丁共 15 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 |
|---|---|---|---|---|---|---|---|---|
| 5034276 | 高危 | January 9, 2024-KB5034276 Cumulative Update for .NET Framework 3.5, 4.8 and 4.8.1 | CVE-2024-21312 | Denial of Service | Important | No | No | 2 |
| | | | CVE-2024-0057 | Security Feature Bypass | Important | No | No | 2 |
| | | | CVE-2024-0056 | Security Feature Bypass | Important | No | No | 2 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | for Windows 11, version 21H2 - Microsoft Support | | | | | | |
| 5034270 | 高危 | January 9, 2024- Security Only Update for .NET Framework 2.0, 3.0, 3.5 SP1, 4.6.2 for Windows Server 2008 SP2 (KB5034270) - Microsoft Support | CVE-2024-0057 | Security Feature Bypass | Important | No | No | 2 |
| | | | CVE-2024-0056 | Security Feature Bypass | Important | No | No | 2 |
| 5034280 | 高危 | January 9, 2024- Security and Quality Rollup for .NET Framework 2.0, 3.0, 3.5 SP1, 4.6.2 for Windows Server 2008 SP2 (KB5034280) - Microsoft Support | CVE-2024-0057 | Security Feature Bypass | Important | No | No | 2 |
| | | | CVE-2024-0056 | Security Feature Bypass | Important | No | No | 2 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 5034279 | 高危 | January 9, 2024- Security and Quality Rollup for .NET Framework 3.5, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Windows Server 2012 R2 (KB5034279) - Microsoft Support | CVE-2024-21312 | Denial of Service | Important | No | No | 2 |
| | | | CVE-2024-0057 | Security Feature Bypass | Important | No | No | 2 |
| | | | CVE-2024-0056 | Security Feature Bypass | Important | No | No | 2 |
| 5034275 | 高危 | January 9, 2024- KB5034275 Cumulative Update for .NET Framework 3.5, 4.8 and 4.8.1 for Windows 10 Version 22H2 - Microsoft Support | CVE-2024-21312 | Denial of Service | Important | No | No | 2 |
| | | | CVE-2024-0057 | Security Feature Bypass | Important | No | No | 2 |
| | | | CVE-2024-0056 | Security Feature Bypass | Important | No | No | 2 |
| 5034272 | 高危 | January 9, 2024- KB5034272 Cumulative Update | CVE-2024-21312 | Denial of Service | Important | No | No | 2 |
| | | | CVE-2024-0057 | Security Feature Bypass | Important | No | No | 2 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | for .NET Framework 3.5, 4.8 and 4.8.1 for Azure Stack HCI, version 22H2 - Microsoft Support | CVE-2024-0056 | Security Feature Bypass | Important | No | No | 2 |
| 5034269 | 高危 | January 9, 2024- 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 (KB5034269) - Microsoft Support | CVE-2024-21312 | Denial of Service | Important | No | No | 2 |
| | | | CVE-2024-0057 | Security Feature Bypass | Important | No | No | 2 |
| | | | CVE-2024-0056 | Security Feature Bypass | Important | No | No | 2 |
| 5033910 | 高危 | January 9, 2024- KB5033910 Cumulative Update | CVE-2024-21312 | Denial of Service | Important | No | No | 2 |
| | | | CVE-2024-0057 | Security Feature Bypass | Important | No | No | 2 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | for .NET Framework 4.8 for Windows 10, version 1607 and Windows Server 2016 - Microsoft Support | CVE-2024-0056 | Security Feature Bypass | Important | No | No | 2 |
| 5034273 | 高危 | January 9, 2024-KB5034273 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-2024-21312 | Denial of Service | Important | No | No | 2 |
| | | | CVE-2024-0057 | Security Feature Bypass | Important | No | No | 2 |
| | | | CVE-2024-0056 | Security Feature Bypass | Important | No | No | 2 |
| 5034277 | 高危 | January 9, 2024-Security and Quality Rollup for .NET Framework 3.5.1, 4.6.2, 4.7, | CVE-2024-0057 | Security Feature Bypass | Important | No | No | 2 |
| | | | CVE-2024-0056 | Security Feature Bypass | Important | No | No | 2 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | 4.7.1, 4.7.2, 4.8 for Windows Embedded 7 Standard and Windows Server 2008 R2 SP1 (KB5034277) - Microsoft Support | | | | | | |
| 5002541 | 高危 | Description of the security update for SharePoint Enterprise Server 2016: January 9, 2024 (KB5002541) - Microsoft Support | CVE-2024-21318 | Remote Code Execution | Important | No | No | 1 |
| 5034278 | 高危 | January 9, 2024- Security and Quality Rollup for .NET Framework 3.5, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 | CVE-2024-21312 | Denial of Service | Important | No | No | 2 |
| | | | CVE-2024-0057 | Security Feature Bypass | Important | No | No | 2 |
| | | | CVE-2024-0056 | Security Feature Bypass | Important | No | No | 2 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | for Windows Server 2012 (KB5034278) - Microsoft Support | | | | | | |
| 5033920 | 高危 | January 9, 2024- KB5033920 Cumulative Update for .NET Framework 3.5 and 4.8.1 for Windows 11, version 22H2 and Windows 11, version 23H2 - Microsoft Support | CVE-2024-21312 | Denial of Service | Important | No | No | 2 |
| | | | CVE-2024-0057 | Security Feature Bypass | Important | No | No | 2 |
| | | | CVE-2024-0056 | Security Feature Bypass | Important | No | No | 2 |
| 5034274 | 高危 | January 9, 2024- KB5034274 Cumulative Update for .NET Framework 3.5, 4.8 and 4.8.1 for Windows 10 Version 21H2 - Microsoft Support | CVE-2024-21312 | Denial of Service | Important | No | No | 2 |
| | | | CVE-2024-0057 | Security Feature Bypass | Important | No | No | 2 |
| | | | CVE-2024-0056 | Security Feature Bypass | Important | No | No | 2 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 5034120 | 高危 | KB5034120: Cumulative security update for Internet Explorer: January 9, 2024 - Microsoft Support | CVE-2024-20652 | Security Feature Bypass | Important | No | No | 1 |

本月发布一般性更新补丁。

| KBID | 奇安信集团级别 | 详细信息 |
|---|---|---|
| 5002500 | 其他功能性补丁 | Office 2016 更新程序 |

注：

1、 上述表格中“漏洞的可利用性”编号详细说明如下：

0 - 已被利用(Exploitation Detected)

1 - 更有可能被利用(Exploitation More Likely)

2 - 不太可能利用(Exploitation Less Likely)

3 - 不可能利用(Exploitation Unlikely)

4 - 不受漏洞的影响(N/A)

# 第5章 参考链接

- Security Update Guide

https://portal.msrc.microsoft.com/zh-cn/security-guidance

- Latest non-security updates for versions of Office that use Windows Installer (MSI)

https://docs.microsoft.com/en-us/OfficeUpdates/office-msi-non-security-updates