预警编号：ENE-P-A-201927

|  |  |  |  |
| --- | --- | --- | --- |
| **重要程度** | 重要 | **紧急程度** | 紧急 |
| **涉及产品** | 安装微软操作系统的华为智能计算服务器 | | |
| **涉及版本** | 参见影响和范围中的华为转售且涉及该漏洞的微软产品列表 | | |
| **涉及应用范围** | 安装了Windows 产品的华为智能计算机架、刀片、高性能、高密、昆仑系列等服务器。 | | |
| **发布时间** | 2019-05-27 | | |
| **预防要求** | A、     描述预防的策略：预警送达/客户培训。  B、     涉及软件可由客户依据业务需要自行决定并实施操作。  C、     完成客户预警送达，并要有送达客户记录。 | | |
| **联系人** | 服务接口人 | 杨凯华 00303081 18926459381 | |
| 研发接口人 | 姚 强 00385768 18010150409 | |

**【问题描述】**

北京时间2019年5月15日，微软公司修复了远程桌面服务（Remote Desktop Services）中的远程代码执行漏洞CVE-2019-0708。未经身份验证的攻击者通过该漏洞，可向目标Windows主机发送恶意构造的请求，在目标系统上执行任意代码，影响客户业务正常运行和数据安全。

**【原因/触发因素】**

远程桌面服务（Remote Desktop Services）中存在一个远程代码执行漏洞。当未经身份验证的攻击者使用RDP连接到目标系统并发送特制请求时可以触发。此漏洞是预身份验证，无需用户交互。成功利用此漏洞的攻击者可以在目标系统上执行任意代码。包括以安装程序，查看、更改或删除数据，或创建具有完全用户权限的新帐户。参考微软官方安全通告： <https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708>

**【影响和风险】**

攻击者通过该漏洞可在目标系统上执行任意代码，如安装程序，查看、更改或删除数据，创建具有完全用户权限的新帐户，影响客户业务正常运行和数据安全。

安装在华为服务器设备上的微软操作系统均存在该风险。

华为转售且涉及该漏洞的微软产品列表：

|  |
| --- |
| 受影响的操作系统版本 |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) |

**【措施和解决方案】**

**规避措施：**

方案一：Windows Server 2008 R2 SP1用户使用windows update自动获取补丁升级：打开Windows Update功能，然后点击“检查更新”按钮，根据业务情况下载安装相关安全补丁。

方案二：参考微软官方安全通告： <https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708>，请客户自行获取对应操作系统安全补丁并手动安装。

**【联系人】**

服务代表信息

运营商客户群 ：何玉春 00430956 18676789038 heyuchun@huawei.com

企业客户群  ：杨凯华 00303081 18926459381 yangkaihua.yang@huawei.com

研发接口人信息

运营商/企业客户群：姚强 00385768 18010150409 yaoqiang4@huawei.com