



紧急安全通知

编号: MAR 4495-1

尊敬的生物梅里埃用户:

安全是梅里埃关心的主要问题。

像大多数其他公司一样,梅里埃使用的系统是基于 Microsoft® Windows 操作系统。我们希望与您分享一些指导,以保护您的梅里埃系统。

梅里埃跟随 Microsoft® Windows 的发展,在您的实验室中,您可能有各种版本的 Microsoft® Windows 操作系统。

Microsoft®在8月13日星期二披露了一个**影响远程桌面服务(RDP)的关键漏洞-以前称为终端服务-嵌入 Windows 操作系统中**。

如果还没有证据表明该漏洞被利用,则此漏洞可能会被用于能够快速跨网络传播的恶意软件中。

由于在世界各地数百万台计算机上有远程桌面服务,因此必须尽快采取适当行动保护梅里埃系统。

问题描述:

远程桌面服务(以前称为终端服务)中存在远程代码执行漏洞-未经身份验证的攻击者使用 RDP 连接到目标系统并发送精心构建的请求。此漏洞是预身份验证,不需要用户交互。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。然后,攻击者可以安装程序;查看、更改或删除数据;或创建具有完整用户权限的新帐户。

要利用此漏洞,攻击者需要通过 RDP 向目标系统远程桌面服务发送精心构建的请求。

bioMérieux (Shanghai) Company Limited/梅里埃诊断产品(上海)有限公司

中国上海市浦东新区康桥工业区浦三路 4633 号 邮编: 201315,
4633 Pusan Road, Kangqiao Industrial Park, Pudong Shanghai, 201315 PRC
电话 Telephone: +86 (21) 60978388 传真 Fax: +86 (21) 60978399 - www.biomerieux.com



需要采取的行动:

受影响的 Microsoft® Windows 操作系统摘要

| 版本 | 是否受影响 |
|--|----------------|
| Windows XP SP0/SP1/SP2 or earlier | 否 |
| Windows Embedded Standard 2009 (XPe SP3) | 否 |
| Windows Embedded Standard 7 SP0 | 潜在受影响，未有微软正式沟通 |
| Windows Embedded Standard 7 SP1 | 是 |
| Windows Server 2008 R2 SP1 | 是 |
| Windows 10 | 是 |
| Windows Server 2016 | 是 |

识别您的操作系统

登录 Windows

按 Windows +中断（也称为“暂停”）键以启动系统属性

检查 Windows

| 版本 | 截图 |
|---------------------------------|----|
| Windows Embedded Standard 7 SP0 | |
| Windows Embedded Standard 7 SP1 | |
| Windows Server 2008 R2 SP1 | |

bioMérieux (Shanghai) Company Limited/梅里埃诊断产品(上海)有限公司

中国上海市浦东新区康桥工业区浦三路 4633 号 邮编: 201315,
4633 Pusan Road, Kangqiao Industrial Park, Pudong Shanghai, 201315 PRC
电话 Telephone: +86 (21) 60978388 传真 Fax: +86 (21) 60978399 - www.biomerieux.com



Microsoft® 发布了哪些版本的更新?

| 版本 | 操作系统支持状态 | Windows 安全更新可用性 | 分配渠道 |
|---------------------------------|----------|-----------------|-----------------|
| Windows Embedded Standard 7 SP0 | 停止支持 | 否 | 不适用 |
| Windows Embedded Standard 7 SP1 | 支持 | 是 | Windows 更新 (标准) |
| Windows Server 2008 R2 SP1 | 支持 | 是 | Windows 更新 (标准) |
| Windows 10 | 支持 | 是 | Windows 更新 (标准) |
| Windows Server 2016 | 支持 | 是 | Windows 更新 (标准) |

推荐

在使用上述 Microsoft® Windows 操作系统列表的梅里埃计算机上，我们建议您使用通常的操作系统更新过程，尽快更新系统：

- 对于 Windows Embedded Standard 7 SP1 和 Windows Server 2008 R2 SP1 : 安装 Aug 2019 Monthly Rollup
- 对于 Windows 10 和 Windows Server 2016: 安装 Aug 2019 Monthly Update

对于上面未列出的所有其他操作系统，Microsoft® 不支持或提供任何安全更新：

- 如果可能，请将计算机与网络隔离(如果计算机仅通过 RS232 连接，则无需断开此端口)。
- 阻止企业外围防火墙上的 TCP 端口 3389(远程桌面协议)。
- 请联系您的梅里埃代表，讨论最适合的行动。

梅里埃致力于为客户提供最优质的产品。如果您有任何问题，请联系您当地的生物梅里埃代表。

感谢您持续使用梅里埃产品。

此致

敬礼

梅里埃诊断产品（上海）有限公司

2019 年 12 月 2 日

bioMérieux (Shanghai) Company Limited/梅里埃诊断产品(上海)有限公司

中国上海市浦东新区康桥工业区浦三路 4633 号 邮编：201315，
4633 Pusan Road, Kangqiao Industrial Park, Pudong Shanghai, 201315 PRC
电话 Telephone: +86 (21) 60978388 传真 Fax: +86 (21) 60978399 - www.biomerieux.com



附录

- 2019年8月13日 Microsoft® 博文
<https://msrc-blog.microsoft.com/2019/08/13/patch-new-wormable-vulnerabilities-in-remote-desktop-services-cve-2019-1181-1182/>
- 2019年8月13日 Microsoft® 关于 CVE-2019-1181 的安全公告
<https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-1181>
- 2019年8月13日 Microsoft® 关于 CVE-2019-1182 的安全公告
<https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-1182>

bioMérieux (Shanghai) Company Limited/梅里埃诊断产品(上海)有限公司

中国上海市浦东新区康桥工业区浦三路 4633 号 邮编: 201315,
4633 Pusan Road, Kangqiao Industrial Park, Pudong Shanghai, 201315 PRC
电话 Telephone: +86 (21) 60978388 传真 Fax: +86 (21) 60978399 - www.biomerieux.com