

2013 年 8 月微软发布的正式补丁

目录

微软发布 2013 年 8 月份的安全公告 2



ANTI-SPYWARE



ANTI-SPAM



WEB REPUTATION



ANTIVIRUS



ANTI-PHISHING



WEB FILTERING

微软发布 2013 年 8 月份的安全公告

微软已经发布了 2013 年 8 月份的安全公告，本次公告共 8 个。

MS13-059

Internet Explorer 的累积性安全更新 (2862772)

漏洞描述:

此安全更新解决 Internet Explorer 中的 11 个秘密报告的漏洞。最严重的漏洞可能在用户使用 Internet Explorer 查看特制网页时允许远程执行代码。成功利用这些最严重的漏洞的攻击者可以获得与当前用户相同的用户权限。那些帐户被配置为拥有较少系统用户权限的用户比具有管理用户权限的用户受到的影响要小。

<http://technet.microsoft.com/zh-cn/security/bulletin/MS13-059>

MS13-060

Unicode 脚本处理器中的漏洞可能允许远程执行代码 (2850869)

漏洞描述:

此安全更新可解决 Microsoft Windows 中的 Unicode 脚本处理器中一个秘密报告的漏洞。如果用户使用支持 Embedded OpenType 字体的应用程序查看特制的文档或网页，此漏洞可能允许远程执行代码。成功利用此漏洞的攻击者可以获得与当前用户相同的用户权限。那些帐户被配置为拥有较少系统用户权限的用户比具有管理用户权限的用户受到的影响要小。

<http://technet.microsoft.com/zh-cn/security/bulletin/MS13-060>

MS13-061

Microsoft Exchange Server 中的漏洞可能允许远程执行代码 (2876063)

漏洞描述:

此安全更新可解决 Microsoft Exchange Server 中公开披露的三个漏洞。Microsoft Exchange Server 的 WebReady Document Viewing 和数据丢失防护功能中存在漏洞。如果用户使用 Outlook Web App (OWA) 预览特制文件，则漏洞可以在 Exchange 服务器上代码转换服务的安全上下文中远程执行代码。Exchange 中用于 WebReady Document Viewing 的代码转换服务使用 LocalService 帐户的凭据。数据丢失防护功能托管如果 Exchange 服务器收到特制邮件则可能允许在筛选管理服务的上下文中远程执行代码的代码。

<http://technet.microsoft.com/zh-cn/security/bulletin/MS13-061>

MS13-062

远程过程调用中的漏洞可能允许特权提升 (2849470)

漏洞描述:



ANTI-SPYWARE



ANTI-SPAM



WEB REPUTATION



ANTIVIRUS



ANTI-PHISHING



WEB FILTERING

此安全更新可解决 Microsoft Windows 中一个秘密报告的漏洞。如果攻击者发送特制 RPC 请求，则该漏洞可能允许特权提升。该安全更新通过更正 Microsoft Windows 处理匿名 RPC 消息的方式来解决漏洞。

<http://technet.microsoft.com/zh-cn/security/bulletin/MS13-062>

MS13-063

Windows 内核中的漏洞可能允许特权提升 (2859537)

漏洞描述:

此安全更新可解决 Microsoft Windows 中一个公开披露的漏洞和三个秘密报告的漏洞。如果攻击者本地登录并运行特制应用程序，最严重的漏洞可能允许特权提升。攻击者必须拥有有效的登录凭据并能本地登录才能利用这些漏洞。匿名用户无法利用这些漏洞，也无法以远程方式利用这些漏洞。

<http://technet.microsoft.com/zh-cn/security/bulletin/MS13-063>

MS13-064

Windows NAT 驱动程序中的漏洞可能允许拒绝服务 (2849568)

漏洞描述:

此安全更新可解决 Microsoft Windows 的 Windows NAT 驱动程序中一个秘密报告的漏洞。如果攻击者向运行 Windows NAT 驱动程序服务的目标服务器发送特制 ICMP 数据包，则该漏洞可能允许拒绝服务。

<http://technet.microsoft.com/zh-cn/security/bulletin/MS13-064>

MS13-065

ICMPv6 中的漏洞可能允许拒绝服务 (2868623)

漏洞描述:

此安全更新可解决 Microsoft Windows 中一个秘密报告的漏洞。如果攻击者向目标系统发送特制 ICMPv6 数据包，则该漏洞可能允许拒绝服务。

<http://technet.microsoft.com/zh-cn/security/bulletin/MS13-065>

MS13-066

Active Directory 联合身份验证服务中的漏洞可能允许信息泄露 (2873872)

漏洞描述:

此安全更新可解决 Active Directory 联合身份验证服务 (AD FS) 中一个秘密报告的漏洞。该漏洞可能泄露与 AD FS 所使用的服务帐户相关的信息。攻击者随后可尝试从公司网络外部登录，这将导致锁定 AD FS 所使用的服务帐户（如果已配置帐户锁定策略）。这将导致依赖 AD FS 实例的所有应用程序出现拒绝服务情形。

<http://technet.microsoft.com/zh-cn/security/bulletin/MS13-066>



ANTI-SPYWARE



ANTI-SPAM



WEB REPUTATION



ANTIVIRUS



ANTI-PHISHING



WEB FILTERING