互联网网络安全信息通报

2017 年第 594 期（总第 1230 期）

国家计算机网络应急技术处理协调中心广东分中心　2017 年 11 月 17 日

关于 Microsoft office 组件 EQNEDT32.EXE 存在内存破坏漏洞的预警通报

近日，国家信息安全漏洞共享平台（CNVD）收录了 Microsoft office 组件 EQNEDT32.EXE 内存破坏漏洞（CNVD-2017-34031，对应 CVE-2017-11882），该漏洞允许未经身份验证的远程攻击者在目标系统上执行恶意代码。微软 office 在过去 17 年中，包括 office 365 在内的所有版本均存在该漏洞，漏洞影响范围极为广泛。

一、漏洞情况分析

2017 年 11 月 14 日，微软发布了安全补丁修复了 office 组件中的一个内存破坏漏洞，该漏洞位于负责在文档中插入和编辑公式（OLE 对象）的 MS 办公室组件 EQNEDT32.EXE 中。由于内存操作不正确，组件无法正确处理内存中的对象，从而使攻击者可以在登录用户的上下文中执行恶意代码。2000 年，微软厂商在 office 2000 中引入了 EQNEDT32EXE，并保存在 office 2007 之后发布的所有版本中，以确保软件与旧版本的文档的兼容性。

利用此漏洞需要使用受影响的微软 office 或 Microsoft 写字板程序打开恶意文件,使未经身份验证的远程攻击者可以在目标系统上执行恶意代码,远程安装恶意软件,进而可能控制整个操作系统。CNVD 对该漏洞的综合评级为“高危”。

二、漏洞影响范围

Microsoft Office 2007 及其以后，包括 office 365 在内的所有 Microsoft office 版本。

三、处置建议

我中心针对上述漏洞建议如下:

1、微软公司已经发布该漏洞的补丁，强烈建议 office 用户尽快更新 11 月的安全补丁，以防止黑客和网络控制他们的计算机。

2、不能及时升级补丁的,可以在命令提示符下运行以下命令,在 Windows 注册表中禁用该组件:

reg add “HKLM\SOFTWARE\Microsoft\Office\Common\COM Compatibility\{0002CE02-0000-0000-C000-000000000046}” /v “Compatibility Flags” /t REG_DWORD /d 0x400

对于 x64 OS 中的 32 位 Microsoft Office 软件包，运行以下命令:

reg add “HKLM\SOFTWARE\Wow6432Node\Microsoft\Office\Common\COM Compatibility\{0002CE02-0000-0000-C000-000000000046}” /v “Compatibility Flags” /t REG_DWORD /d 0x400

此外，用户还应启用Microsoft Office 沙箱等以防止活动内容执行 (OLE/ActiveX/Macro)。

附：参考链接：

https://thehackernews.com/2017/11/microsoft-office-rce-exploit.html

http://www.cnvd.org.cn/flaw/show/CNVD-2017-34031

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11882 (微软官方安全建议)

联系电话：020-85526437

电子邮箱：gd@cert.org.cn