预警编号：YJ-2017030

恒安嘉新

关于 Microsoft office 组件

EQNEDT32.EXE 存在内存破坏漏洞

安全预警通告

恒安嘉新（北京）科技股份公司

2017 年 11 月 16 日

1 漏洞描述

近期，互联网爆出 Microsoft office 组件 EQNEDT32.EXE 内存破坏漏洞(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。漏洞危害程度为高危(High)。

2 影响范围

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

3 漏洞原理

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。

4 修复建议

1）微软公司已经发布该漏洞的补丁，鉴于该漏洞广泛存在，且易于被用于发起网络攻击，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）另，不能及时更新安全补丁的用户，可采取如下临时解决方案

用户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\COMCompatibility\{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)。