微软 11 月升级提示通告

升级提示通告

奇安信 CERT 监测到 11 月 11 日微软共发布了 112 个漏洞的补丁程序，其中，Windows Kernel、Windows Network File System、Microsoft Exchange Server、Windows Print Spooler、Microsoft SharePoint、Windows Hyper-V 等产品中的 17 个漏洞被微软官方标记为紧急漏洞。经研判，以下 8 个漏洞（包括 2 个紧急漏洞和 6 个重要漏洞）影响较大。另外，CVE-2020-17051、CVE-2020-17052、CVE-2020-17053、CVE-2020-16998、CVE-2020-17010、CVE-2020-17038、CVE-2020-17057、CVE-2020-17056、CVE-2020-17061、CVE-2020-17088 漏洞被微软标记为 “Exploitation More Likely”，这代表这些漏洞更容易被利用。鉴于这些漏洞危害较大，建议客户尽快安装更新补丁。

发布时间

官方通告发布日期	2020-11-10
奇安信 CERT 通告日期	2020-11-11

重点关注漏洞

漏洞编号	CVSS	概述	影响版本
CVE-2020-17051	9.8	Windows 网络文件系统（NFS）的远程代码执行漏洞。NFS 是一种文件系统协议，用于跨网络上的多个操作系统共享文件。该漏洞会影响 Windows 的所有受支持版本，CVSS 评分 9.8，无需身份验证或用户交互即可加以利用。据国外分析文章指出，CVE-2020-17051 与 CVE-2020-17056（NFS 中的一个远程内核数据读取漏洞）相结合，以绕过地址空间布局随机化（ASLR），这可能会增加远程利用的可能性，且如果 NFS 已配置为允许匿名写访问，则利用 CVE-2020-17051 漏洞可能造成网络蠕虫。	影响版本见以下链接：https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17051
CVE-2020-17042	8.8	Windows Print Spooler 中的 RCE 漏洞。CVSS 评分为 8.8，但该漏洞的可利用性等级为“Exploitation Less Likely”。微软官方没有提供有关漏洞或要利用的条件的任何详细信息，考虑到 Windows Print Spooler 历史漏洞，将 Windows Print Spooler 中的漏洞与其他漏洞联系在一起，打印后台处理程序作为一种攻击媒介，可实现控制主机权限并进一步在网络中传播。	影响版本见以下链接：https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17042
CVE-2020-17087	7.8	Windows 内核密码驱动程序 cng.sys 中的特权提升漏洞，已作为 CVE-2020-15999（FreeType 2 库中的缓冲区溢出漏洞）的漏洞链的一部分被广泛利用。CVE-2020-17087 被用于	影响版本见以下链接：https://portal.msrc.microsoft.com/en-US/security-

漏洞编号	CVSS	概述	影响版本
		逃脱 Google Chrome 浏览器的沙箱，以提升被利用系统的特权，且目前该漏洞已被在野利用。	guidance/advisory/CVE-2020-17087
CVE-2020-17056	5.5	CVE-2020-17056 是 NFS 中的一个远程内核数据读取漏洞，以绕过地址空间布局随机化（ASLR），与 CVE-2020-17051 相结合会增加远程利用的可能性。	影响版本见以下链接：https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17056
CVE-2020-17061	8.8	Microsoft SharePoint 中的远程代码执行漏洞。远程攻击者可以利用此漏洞在 SharePoint 服务器上获得代码执行权限。但攻击者需要低权限才能利用此漏洞。	影响版本见以下链接：https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ CVE-2020-17061
CVE-2020-17083 CVE-2020-17084	5.5 8.5	CVE-2020-17083 和 CVE-2020-17084 都是 Microsoft Exchange Server 中的 RCE 漏洞。多年来，Microsoft Exchange 一直是攻击者的重要目标，而 Exchange 服务器修补速度缓慢已导致针对多个组织的成功攻击。CVE-2020-17083 的 CVSS 评分为 5.5，而 CVE-2020-17084 的 CVSS 评分为 8.5。尽管两个漏洞都被标记为“不太可能利用”，但通过查看 CVSS 评分数据，很可能可以通过诱使用户打开精心构造的电子邮件来利用这些漏洞。据国外研究人员指出，这两个漏洞可能与 CVE-2020-16875 补丁绕过有关。	影响版本见以下链接：https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17083 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17084
CVE-2020-17040	6.5	Windows Hyper-V 中存在一枚安全功能绕过漏洞。目前尚不清楚会绕过 Hyper-V 中的哪个安全功能，以及攻击者如何利用它。但是攻击的复杂度	影响版本见以下链接：https://portal.msrc.microsoft.com/en-US/security-

漏洞编号	CVSS	概述	影响版本
		很低，无需身份验证及用户交互。仅通过标题和 CVSS 评分看此漏洞值得关注。	guidance/advisory/CVE-2020-17040
更多漏洞可前往参考链接查看			

修复方法

请参考以下链接安装补丁更新：

https://msrc.microsoft.com/update-guide/releaseNote/2020-Nov

参考链接

https://msrc.microsoft.com/update-guide/releaseNote/2020-Nov

奇安信 CERT

【我们是谁】

奇安信应急响应部（又称：奇安信 CERT，奇安信 A-TEAM）成立于 2016 年，是属于奇安信旗下的网络安全应急响应平台，平台旨在第一时间为客户提供漏洞或网络安全事件安全风险通告、响应处置建议、相关技术和奇安信相关产品的解决方案。

奇安信 A-TEAM：团队主要致力于 Web 渗透、APT 攻防、对抗，前瞻性攻防工具预研。从底层原理、协议层面进行严肃、有深度的技术研究，深入还原攻与防的技术本质，曾多次率先披露 Windows 域、Exchange、WebLogic、Exim 等重大安全漏洞，第一时间发布相关漏洞风险通告及可行的处置措施并获得官方致谢。欢迎有意者加入！

【我们的服务】

安全风险通告：奇安信 CERT 成立至今已发布上百篇安全风险通告，从成立至今，针对多个高危漏洞、网络安全事件发布风险通告并给出了有效的安全措施。我们的安全研究团队将实时跟踪安全热点事件和漏洞，始终站在用户的视角去评估风险，致力于第一时间向客户发送有效的风险和相关解决方案。

【订阅方式】

发送接收邮箱和所属单位至：cert@qianxin.com

【微信公众号】

奇安信 CERT