关于对部分重要漏洞进行安全加固的预警通报

国家网络与信息安全信息通报中心组织有关技术支持单位，对近两年曝光且影响广泛的重要漏洞进行了梳理。截至目前，此类漏洞仍在各重要信息系统中普遍存在。建议各成员单位组织本行业、本单位开展自查自排，及时采取整改加固措施，确保国庆 70 周年期间网络与信息安全。主要漏洞有：

一、Windows 远程桌面服务远程代码执行漏洞（CVE-2019-0708）

漏洞介绍：

未经身份认证的攻击者可通过 RDP 协议链接到目标系统并发送精心构造的请求可触发此漏洞。成功利用此漏洞时可执行任意代码。此漏洞易被蠕虫病毒制造者利用。

影响范围：

主要影响 Windows7、Window Server 2008、Windows2003、WindowXP 操作系统。

漏洞修复方案：

请参考以下官方安全通告下载并安装最新补丁：

- https://support.microsoft.com/zh-cn/help/4500705/customer-guidance-for-cve-2019-0708
- https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708

二、微软远程桌面服务远程代码执行漏洞（CVE-2019-1181/1182）

漏洞介绍：

攻击者可通过 RDP 向目标系统远程桌面服务发送精心构造的请求，成功利用该漏洞时可以在目标系统上执行任意代码。

影响范围：

此漏洞影响版本较多，请查看官方说明。

漏洞修复方案：

请参考以下官方安全通告下载并安装最新补丁：

- https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1182
- https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1181

三、Windows 认证漏洞（CVE-2019-1040）

漏洞介绍：

此漏洞可造成多种不同的危害，严重时攻击者可以在仅有一个普通域账号的情况下远程控制 Windows 域内的任何机器，包括域控服务器。

影响范围：

此漏洞影响版本较多，请查看官方说明。

漏洞修复方案：

请在所有受影响的 Windows 客户端、服务器下载安装更新，安装完毕后需重启服务器。：

- https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1040

四、Exchange SSRF 漏洞（CVE-2018-8581）

漏洞介绍：

攻击者在拥有目标网络内任意邮箱权限或者已控制目标网络内的任意一台与域内机器在同一网段的机器，并成功针对域内机器发起 windows name resolution spoofing 攻击时可触发此漏洞时，可直接控制目标网络内所有的 Windows 机器。

影响范围：

Microsoft Exchange Server 2010、2013、2016、2019

漏洞修复方案：

请参考以下官方安全通告下载并安装最新补丁：

- https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0686

五、Oracle WebLogic 远程代码执行漏洞（CVE-2019-2729）

漏洞介绍：

攻击者可利用此漏洞绕过 CVE-2019-2725 的补丁，造成远程任意代码执行漏洞。并且此漏洞不受 JDK 版本的影响。

影响范围：

Oracle WebLogic 10.3.6、12.1.3、12.2.1.3

漏洞修复方案：

官方已发布相关更新补丁，请安装更新进行修复。

六、ThinkPHP 5.x 远程代码执行漏洞

漏洞介绍：

ThinkPHP 对控制器没有做到足够的检测，导致 Pathinfo 在访问模式时，可能 Getshell。

影响范围：

ThinkPHP 5.1.x < 5.1.31

ThinkPHP 5.0.x < 5.0.23

漏洞修复方案：

- 更新 ThinkPHP 5.0.X 到 ThinkPHP 5.0.23

http://www.thinkphp.cn/down/1278.html

- 更新 ThinkPHP 5.1.x 到 ThinkPHP 5.1.31

https://github.com/top-think/framework/commit/adde39c236cfeda454fe725d999d89abf67b8caf

七、FastJson 远程代码执行漏洞

漏洞介绍：

攻击者可以通过提交精心构造的 JSON 数据实现远程代码

执行。

影响范围：

FastJson < 1.2.48

漏洞修复方案：

FastJson 升级到 1.2.51

FastJson 升级到 1.2.58

八、VxWorks 多个高危漏洞

漏洞介绍：

VxWorks 系统（广泛用于工业、医疗和企业设备中，使用量超过 20 亿）存在 6 个严重漏洞可远程执行代码：CVE-2019-12255 、 CVE-2019-12256 、 CVE-2019-12257 、CVE-2019-12260、CVE-2019-12261、CVE-2019-12263。

影响范围：

漏洞影响版本较多，请参考修复方案。

漏洞修复方案：

下载安装补丁或更新到最新版本：

- https://support2.windriver.com/index.php?page=cve&on=view&id=CVE-2019-12255
- https://support2.windriver.com/index.php?page=cve&on=view&id=CVE-2019-12256
- https://support2.windriver.com/index.php?page=cve&on=view&id=CVE-2019-12257

- https://support2.windriver.com/index.php?page=cve&on=view&id=CVE-2019-12260
- https://support2.windriver.com/index.php?page=cve&on=view&id=CVE-2019-12261

https://support2.windriver.com/index.php?page=cve&on=view&id=CVE-2019-12263