## 192.168.59.35

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1 | 13 | 28 | 1 | 77 |
| **紧急** | **高危** | **中危** | **低危** | **信息** |

详细信息：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 紧急 | 名称 | CVE | CVSS | protocol | port |
| Critical | MS14-066: Schannel 中的漏洞可能允许远程代码执行(2992611)(未授权检查) | CVE-2014-6321 | 10.0 | tcp | 3389 |
| **漏洞描述：**由于安全通道(Schannel)安全包对数据包的处理不当，远程 Windows 主机受到远程代码执行漏洞的影响。攻击者可以通过向 Windows 服务器发送特制的包来利用这个问题。注意，这个插件发送一个客户端证书 TLS 握手消息，然后是 CertificateVerify 消息。一些 Windows 主机在接收到客户端证书时将关闭连接，而它并没有通过 CertificateRequest 消息请求客户端证书。在这种情况下，插件无法继续检测漏洞，因为 CertificateVerify 消息无法发送。 | | | | | |
| **加固建议：**微软已经为 Windows 2003，Vista，2008,7,2008 r 2,8,2012,8.1和2012 r 2发布了一系列补丁。 | | | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 高危 | 名称 | CVE | CVSS | protocol | port |
| High | Apache Tomcat 7.0. x < 7.0.57多重漏洞(POODLE) | CVE-2014-3505 | 7.5 | tcp | 8080 |
| **漏洞描述：**根据其自我报告的版本号，监听远程主机的 Apache Tomcat 服务在7.0.57之前是7.0.x。因此，它受到以下漏洞的影响:-d 1both.c 中存在一个内存双空闲错误，该错误与处理允许分布式拒绝服务攻击攻击的 DTLS 数据包有关。(CVE-2014-3505)-d 1 \_ both.c’中存在一个未指明的错误，该错误与处理 DTLS 握手消息有关，由于消耗了大量内存，它允许分布式拒绝服务攻击攻击。(CVE-2014-3506)-一个内存泄漏错误存在于’1both.c’中，这个错误与处理允许分布式拒绝服务攻击攻击的特制 DTLS 数据包有关。(CVE-2014-3507)-当使用各种“ X509 \_ name \_ \*”漂亮的打印函数时，“ OBJ \_ obj2txt”函数中存在错误，从而泄漏了进程堆栈数据，导致信息泄露。(CVE-2014-3508)-存在一个与“ ec 点格式扩展”处理和多线程客户机有关的错误，该客户机允许在恢复会话期间覆盖释放的内存。(CVE-2014-3509)-NULL 指针解引用错误存在于处理匿名 ECDH 密码套件和精心制作的握手消息，这些消息允许针对客户机的分布式拒绝服务攻击攻击。(CVE-2014-3510)-一个错误与处理片段化的“ ClientHello”消息有关，它允许中间的攻击者强制使用 TLS 1.0，而不管服务器和客户机支持更高的协议级别。(CVE-2014-3511)-缓冲区溢出错误存在于与处理安全远程密码协议(SRP)参数相关的‘ SRP \_ lib.c’中，这可能导致分布式拒绝服务攻击溢出或其他未指定的影响。(CVE-2014-3512)-内存泄漏问题存在于与 DTLS SRTP 扩展处理和特殊精心制作的允许分布式拒绝服务攻击攻击的握手消息有关的 d 1 \_ SRTP’中。(CVE-2014-3513)-在使用密码块链接(CBC)模式的块密码加密器加密的消息解密时，SSL 3.0处理填充字节的方式存在错误。如果中间人攻击者能够强制受害者应用程序通过新创建的 SSL 3.0连接重复发送相同的数据，那么他们只需尝试256次就可以解密密文的选定字节。这也被称为贵宾犬问题。(CVE-2014-3566)-在‘ t1 \_ lib.c’中存在一个内存泄漏问题，这个问题与允许分布式拒绝服务攻击攻击的会话票处理有关。(CVE-2014-3567)-与构建配置过程和“ no-ssl3”构建选项有关的错误，该选项允许服务器和客户端处理不安全的 SSL 3.0握手消息。(CVE-2014-3568)-一个 NULL 指针解引用错误存在于‘ t1 \_ lib.c’中，与处理安全远程密码协议(SRP) ServerHello 消息有关，它允许恶意服务器崩溃客户端，导致分布式拒绝服务攻击。(CVE-2014-5139)注意，Nessus 并没有尝试利用这些问题，而是仅仅依赖于应用程序的自我报告版本号。 | | | | | |
| **加固建议：**升级到 Apache Tomcat 7.0.57或更高版本。 | | | | | |
| High | Apache Tomcat 7.0. x < 7.0.57多重漏洞(POODLE) | CVE-2014-3506 | 7.5 | tcp | 8080 |
| **漏洞描述：**根据其自我报告的版本号，监听远程主机的 Apache Tomcat 服务在7.0.57之前是7.0.x。因此，它受到以下漏洞的影响:-d 1both.c 中存在一个内存双空闲错误，该错误与处理允许分布式拒绝服务攻击攻击的 DTLS 数据包有关。(CVE-2014-3505)-d 1 \_ both.c’中存在一个未指明的错误，该错误与处理 DTLS 握手消息有关，由于消耗了大量内存，它允许分布式拒绝服务攻击攻击。(CVE-2014-3506)-一个内存泄漏错误存在于’1both.c’中，这个错误与处理允许分布式拒绝服务攻击攻击的特制 DTLS 数据包有关。(CVE-2014-3507)-当使用各种“ X509 \_ name \_ \*”漂亮的打印函数时，“ OBJ \_ obj2txt”函数中存在错误，从而泄漏了进程堆栈数据，导致信息泄露。(CVE-2014-3508)-存在一个与“ ec 点格式扩展”处理和多线程客户机有关的错误，该客户机允许在恢复会话期间覆盖释放的内存。(CVE-2014-3509)-NULL 指针解引用错误存在于处理匿名 ECDH 密码套件和精心制作的握手消息，这些消息允许针对客户机的分布式拒绝服务攻击攻击。(CVE-2014-3510)-一个错误与处理片段化的“ ClientHello”消息有关，它允许中间的攻击者强制使用 TLS 1.0，而不管服务器和客户机支持更高的协议级别。(CVE-2014-3511)-缓冲区溢出错误存在于与处理安全远程密码协议(SRP)参数相关的‘ SRP \_ lib.c’中，这可能导致分布式拒绝服务攻击溢出或其他未指定的影响。(CVE-2014-3512)-内存泄漏问题存在于与 DTLS SRTP 扩展处理和特殊精心制作的允许分布式拒绝服务攻击攻击的握手消息有关的 d 1 \_ SRTP’中。(CVE-2014-3513)-在使用密码块链接(CBC)模式的块密码加密器加密的消息解密时，SSL 3.0处理填充字节的方式存在错误。如果中间人攻击者能够强制受害者应用程序通过新创建的 SSL 3.0连接重复发送相同的数据，那么他们只需尝试256次就可以解密密文的选定字节。这也被称为贵宾犬问题。(CVE-2014-3566)-在‘ t1 \_ lib.c’中存在一个内存泄漏问题，这个问题与允许分布式拒绝服务攻击攻击的会话票处理有关。(CVE-2014-3567)-与构建配置过程和“ no-ssl3”构建选项有关的错误，该选项允许服务器和客户端处理不安全的 SSL 3.0握手消息。(CVE-2014-3568)-一个 NULL 指针解引用错误存在于‘ t1 \_ lib.c’中，与处理安全远程密码协议(SRP) ServerHello 消息有关，它允许恶意服务器崩溃客户端，导致分布式拒绝服务攻击。(CVE-2014-5139)注意，Nessus 并没有尝试利用这些问题，而是仅仅依赖于应用程序的自我报告版本号。 | | | | | |
| **加固建议：**升级到 Apache Tomcat 7.0.57或更高版本。 | | | | | |
| High | Apache Tomcat 7.0. x < 7.0.57多重漏洞(POODLE) | CVE-2014-3507 | 7.5 | tcp | 8080 |
| **漏洞描述：**根据其自我报告的版本号，监听远程主机的 Apache Tomcat 服务在7.0.57之前是7.0.x。因此，它受到以下漏洞的影响:-d 1both.c 中存在一个内存双空闲错误，该错误与处理允许分布式拒绝服务攻击攻击的 DTLS 数据包有关。(CVE-2014-3505)-d 1 \_ both.c’中存在一个未指明的错误，该错误与处理 DTLS 握手消息有关，由于消耗了大量内存，它允许分布式拒绝服务攻击攻击。(CVE-2014-3506)-一个内存泄漏错误存在于’1both.c’中，这个错误与处理允许分布式拒绝服务攻击攻击的特制 DTLS 数据包有关。(CVE-2014-3507)-当使用各种“ X509 \_ name \_ \*”漂亮的打印函数时，“ OBJ \_ obj2txt”函数中存在错误，从而泄漏了进程堆栈数据，导致信息泄露。(CVE-2014-3508)-存在一个与“ ec 点格式扩展”处理和多线程客户机有关的错误，该客户机允许在恢复会话期间覆盖释放的内存。(CVE-2014-3509)-NULL 指针解引用错误存在于处理匿名 ECDH 密码套件和精心制作的握手消息，这些消息允许针对客户机的分布式拒绝服务攻击攻击。(CVE-2014-3510)-一个错误与处理片段化的“ ClientHello”消息有关，它允许中间的攻击者强制使用 TLS 1.0，而不管服务器和客户机支持更高的协议级别。(CVE-2014-3511)-缓冲区溢出错误存在于与处理安全远程密码协议(SRP)参数相关的‘ SRP \_ lib.c’中，这可能导致分布式拒绝服务攻击溢出或其他未指定的影响。(CVE-2014-3512)-内存泄漏问题存在于与 DTLS SRTP 扩展处理和特殊精心制作的允许分布式拒绝服务攻击攻击的握手消息有关的 d 1 \_ SRTP’中。(CVE-2014-3513)-在使用密码块链接(CBC)模式的块密码加密器加密的消息解密时，SSL 3.0处理填充字节的方式存在错误。如果中间人攻击者能够强制受害者应用程序通过新创建的 SSL 3.0连接重复发送相同的数据，那么他们只需尝试256次就可以解密密文的选定字节。这也被称为贵宾犬问题。(CVE-2014-3566)-在‘ t1 \_ lib.c’中存在一个内存泄漏问题，这个问题与允许分布式拒绝服务攻击攻击的会话票处理有关。(CVE-2014-3567)-与构建配置过程和“ no-ssl3”构建选项有关的错误，该选项允许服务器和客户端处理不安全的 SSL 3.0握手消息。(CVE-2014-3568)-一个 NULL 指针解引用错误存在于‘ t1 \_ lib.c’中，与处理安全远程密码协议(SRP) ServerHello 消息有关，它允许恶意服务器崩溃客户端，导致分布式拒绝服务攻击。(CVE-2014-5139)注意，Nessus 并没有尝试利用这些问题，而是仅仅依赖于应用程序的自我报告版本号。 | | | | | |
| **加固建议：**升级到 Apache Tomcat 7.0.57或更高版本。 | | | | | |
| High | Apache Tomcat 7.0. x < 7.0.57多重漏洞(POODLE) | CVE-2014-3508 | 7.5 | tcp | 8080 |
| **漏洞描述：**根据其自我报告的版本号，监听远程主机的 Apache Tomcat 服务在7.0.57之前是7.0.x。因此，它受到以下漏洞的影响:-d 1both.c’中存在一个内存双空闲错误，该错误与处理允许分布式拒绝服务攻击攻击的 DTLS 数据包有关。(CVE-2014-3505)-d 1 \_ both.c’中存在一个未指明的错误，该错误与处理 DTLS 握手消息有关，由于消耗了大量内存，它允许分布式拒绝服务攻击攻击。(CVE-2014-3506)-内存泄漏错误存在于’1both.c’处理特别制作的 DTLS 数据包，允许分布式拒绝服务攻击攻击。(CVE-2014-3507)-当使用各种“ X509 \_ name \_ \*”漂亮的打印函数时，“ OBJ \_ obj2txt”函数中存在一个错误，从而泄露了进程堆栈数据，导致信息泄露。(CVE-2014-3508)-存在一个与“ ec 点格式扩展”处理和多线程客户机有关的错误，该客户机允许在恢复会话期间覆盖释放的内存。(CVE-2014-3509)-NULL 指针解引用错误存在于处理匿名 ECDH 密码套件和精心制作的握手消息中，这些消息允许针对客户机的分布式拒绝服务攻击攻击。(CVE-2014-3510)-一个错误存在于处理片段化的“ ClientHello”消息中，它允许中间的攻击者强制使用 TLS 1.0，而不管服务器和客户机支持更高的协议级别。(CVE-2014-3511)-缓冲区溢出错误存在于与处理安全远程密码协议(SRP)参数相关的‘ SRP \_ lib.c’中，这可能导致分布式拒绝服务攻击溢出或其他未指定的影响。(CVE-2014-3512)-内存泄漏问题存在于与 DTLS SRTP 扩展处理和特殊制作的允许分布式拒绝服务攻击攻击的握手消息有关的 d 1 \_ SRTP’中。(CVE-2014-3513)-在使用密码块链接(CBC)模式的块密码加密器加密的消息解密时，SSL 3.0处理填充字节的方式存在错误。如果中间人攻击者能够强制受害者应用程序通过新创建的 SSL 3.0连接重复发送相同的数据，那么他们只需尝试256次就可以解密密文的选定字节。这也被称为贵宾犬问题。(CVE-2014-3566)-在‘ t1 \_ lib.c’中存在一个内存泄漏问题，这个问题与允许分布式拒绝服务攻击攻击的会话票据处理有关。(CVE-2014-3567)-与构建配置过程和“ no-ssl3”构建选项有关的错误，该选项允许服务器和客户端处理不安全的 SSL 3.0握手消息。(CVE-2014-3568)-一个 NULL 指针解引用错误存在于‘ t1 \_ lib.c’中，与处理安全远程密码协议(SRP) ServerHello 消息有关，它允许恶意服务器崩溃客户端，导致分布式拒绝服务攻击。(CVE-2014-5139)注意，Nessus 并没有尝试利用这些问题，而是仅仅依赖于应用程序的自我报告版本号。 | | | | | |
| **加固建议：**升级到 Apache Tomcat 7.0.57或更高版本。 | | | | | |
| High | Apache Tomcat 7.0. x < 7.0.57多重漏洞(POODLE) | CVE-2014-3509 | 7.5 | tcp | 8080 |
| **漏洞描述：**根据其自我报告的版本号，监听远程主机的 Apache Tomcat 服务在7.0.57之前是7.0.x。因此，它受到以下漏洞的影响:-d 1both.c 中存在一个内存双空闲错误，该错误与处理允许分布式拒绝服务攻击攻击的 DTLS 数据包有关。(CVE-2014-3505)-d 1 \_ both.c’中存在一个未指明的错误，该错误与处理 DTLS 握手消息有关，由于消耗了大量内存，它允许分布式拒绝服务攻击攻击。(CVE-2014-3506)-一个内存泄漏错误存在于’1both.c’中，这个错误与处理允许分布式拒绝服务攻击攻击的特制 DTLS 数据包有关。(CVE-2014-3507)-当使用各种“ X509 \_ name \_ \*”漂亮的打印函数时，“ OBJ \_ obj2txt”函数中存在错误，从而泄漏了进程堆栈数据，导致信息泄露。(CVE-2014-3508)-存在一个与“ ec 点格式扩展”处理和多线程客户机有关的错误，该客户机允许在恢复会话期间覆盖释放的内存。(CVE-2014-3509)-NULL 指针解引用错误存在于处理匿名 ECDH 密码套件和精心制作的握手消息，这些消息允许针对客户机的分布式拒绝服务攻击攻击。(CVE-2014-3510)-一个错误与处理片段化的“ ClientHello”消息有关，它允许中间的攻击者强制使用 TLS 1.0，而不管服务器和客户机支持更高的协议级别。(CVE-2014-3511)-缓冲区溢出错误存在于与处理安全远程密码协议(SRP)参数相关的‘ SRP \_ lib.c’中，这可能导致分布式拒绝服务攻击溢出或其他未指定的影响。(CVE-2014-3512)-内存泄漏问题存在于与 DTLS SRTP 扩展处理和特殊精心制作的允许分布式拒绝服务攻击攻击的握手消息有关的 d 1 \_ SRTP’中。(CVE-2014-3513)-在使用密码块链接(CBC)模式的块密码加密器加密的消息解密时，SSL 3.0处理填充字节的方式存在错误。如果中间人攻击者能够强制受害者应用程序通过新创建的 SSL 3.0连接重复发送相同的数据，那么他们只需尝试256次就可以解密密文的选定字节。这也被称为贵宾犬问题。(CVE-2014-3566)-在‘ t1 \_ lib.c’中存在一个内存泄漏问题，这个问题与允许分布式拒绝服务攻击攻击的会话票处理有关。(CVE-2014-3567)-与构建配置过程和“ no-ssl3”构建选项有关的错误，该选项允许服务器和客户端处理不安全的 SSL 3.0握手消息。(CVE-2014-3568)-一个 NULL 指针解引用错误存在于‘ t1 \_ lib.c’中，与处理安全远程密码协议(SRP) ServerHello 消息有关，它允许恶意服务器崩溃客户端，导致分布式拒绝服务攻击。(CVE-2014-5139)注意，Nessus 并没有尝试利用这些问题，而是仅仅依赖于应用程序的自我报告版本号。 | | | | | |
| **加固建议：**升级到 Apache Tomcat 7.0.57或更高版本。 | | | | | |
| High | Apache Tomcat 7.0. x < 7.0.57多重漏洞(POODLE) | CVE-2014-3510 | 7.5 | tcp | 8080 |
| **漏洞描述：**根据其自我报告的版本号，监听远程主机的 Apache Tomcat 服务在7.0.57之前是7.0.x。因此，它受到以下漏洞的影响:-d 1both.c 中存在一个内存双空闲错误，该错误与处理允许分布式拒绝服务攻击攻击的 DTLS 数据包有关。(CVE-2014-3505)-d 1 \_ both.c’中存在一个未指明的错误，该错误与处理 DTLS 握手消息有关，由于消耗了大量内存，它允许分布式拒绝服务攻击攻击。(CVE-2014-3506)-一个内存泄漏错误存在于’1both.c’中，这个错误与处理允许分布式拒绝服务攻击攻击的特制 DTLS 数据包有关。(CVE-2014-3507)-当使用各种“ X509 \_ name \_ \*”漂亮的打印函数时，“ OBJ \_ obj2txt”函数中存在错误，从而泄漏了进程堆栈数据，导致信息泄露。(CVE-2014-3508)-存在一个与“ ec 点格式扩展”处理和多线程客户机有关的错误，该客户机允许在恢复会话期间覆盖释放的内存。(CVE-2014-3509)-NULL 指针解引用错误存在于处理匿名 ECDH 密码套件和精心制作的握手消息，这些消息允许针对客户机的分布式拒绝服务攻击攻击。(CVE-2014-3510)-一个错误与处理片段化的“ ClientHello”消息有关，它允许中间的攻击者强制使用 TLS 1.0，而不管服务器和客户机支持更高的协议级别。(CVE-2014-3511)-缓冲区溢出错误存在于与处理安全远程密码协议(SRP)参数相关的‘ SRP \_ lib.c’中，这可能导致分布式拒绝服务攻击溢出或其他未指定的影响。(CVE-2014-3512)-内存泄漏问题存在于与 DTLS SRTP 扩展处理和特殊精心制作的允许分布式拒绝服务攻击攻击的握手消息有关的 d 1 \_ SRTP’中。(CVE-2014-3513)-在使用密码块链接(CBC)模式的块密码加密器加密的消息解密时，SSL 3.0处理填充字节的方式存在错误。如果中间人攻击者能够强制受害者应用程序通过新创建的 SSL 3.0连接重复发送相同的数据，那么他们只需尝试256次就可以解密密文的选定字节。这也被称为贵宾犬问题。(CVE-2014-3566)-在‘ t1 \_ lib.c’中存在一个内存泄漏问题，这个问题与允许分布式拒绝服务攻击攻击的会话票处理有关。(CVE-2014-3567)-与构建配置过程和“ no-ssl3”构建选项有关的错误，该选项允许服务器和客户端处理不安全的 SSL 3.0握手消息。(CVE-2014-3568)-一个 NULL 指针解引用错误存在于‘ t1 \_ lib.c’中，与处理安全远程密码协议(SRP) ServerHello 消息有关，它允许恶意服务器崩溃客户端，导致分布式拒绝服务攻击。(CVE-2014-5139)注意，Nessus 并没有尝试利用这些问题，而是仅仅依赖于应用程序的自我报告版本号。 | | | | | |
| **加固建议：**升级到 Apache Tomcat 7.0.57或更高版本。 | | | | | |
| High | Apache Tomcat 7.0. x < 7.0.57多重漏洞(POODLE) | CVE-2014-3511 | 7.5 | tcp | 8080 |
| **漏洞描述：**根据其自我报告的版本号，监听远程主机的 Apache Tomcat 服务在7.0.57之前是7.0.x。因此，它受到以下漏洞的影响:-d 1both.c 中存在一个内存双空闲错误，该错误与处理允许分布式拒绝服务攻击攻击的 DTLS 数据包有关。(CVE-2014-3505)-d 1 \_ both.c’中存在一个未指明的错误，该错误与处理 DTLS 握手消息有关，由于消耗了大量内存，它允许分布式拒绝服务攻击攻击。(CVE-2014-3506)-一个内存泄漏错误存在于’1both.c’中，这个错误与处理允许分布式拒绝服务攻击攻击的特制 DTLS 数据包有关。(CVE-2014-3507)-当使用各种“ X509 \_ name \_ \*”漂亮的打印函数时，“ OBJ \_ obj2txt”函数中存在错误，从而泄漏了进程堆栈数据，导致信息泄露。(CVE-2014-3508)-存在一个与“ ec 点格式扩展”处理和多线程客户机有关的错误，该客户机允许在恢复会话期间覆盖释放的内存。(CVE-2014-3509)-NULL 指针解引用错误存在于处理匿名 ECDH 密码套件和精心制作的握手消息，这些消息允许针对客户机的分布式拒绝服务攻击攻击。(CVE-2014-3510)-一个错误与处理片段化的“ ClientHello”消息有关，它允许中间的攻击者强制使用 TLS 1.0，而不管服务器和客户机支持更高的协议级别。(CVE-2014-3511)-缓冲区溢出错误存在于与处理安全远程密码协议(SRP)参数相关的‘ SRP \_ lib.c’中，这可能导致分布式拒绝服务攻击溢出或其他未指定的影响。(CVE-2014-3512)-内存泄漏问题存在于与 DTLS SRTP 扩展处理和特殊精心制作的允许分布式拒绝服务攻击攻击的握手消息有关的 d 1 \_ SRTP’中。(CVE-2014-3513)-在使用密码块链接(CBC)模式的块密码加密器加密的消息解密时，SSL 3.0处理填充字节的方式存在错误。如果中间人攻击者能够强制受害者应用程序通过新创建的 SSL 3.0连接重复发送相同的数据，那么他们只需尝试256次就可以解密密文的选定字节。这也被称为贵宾犬问题。(CVE-2014-3566)-在‘ t1 \_ lib.c’中存在一个内存泄漏问题，这个问题与允许分布式拒绝服务攻击攻击的会话票处理有关。(CVE-2014-3567)-与构建配置过程和“ no-ssl3”构建选项有关的错误，该选项允许服务器和客户端处理不安全的 SSL 3.0握手消息。(CVE-2014-3568)-一个 NULL 指针解引用错误存在于‘ t1 \_ lib.c’中，与处理安全远程密码协议(SRP) ServerHello 消息有关，它允许恶意服务器崩溃客户端，导致分布式拒绝服务攻击。(CVE-2014-5139)注意，Nessus 并没有尝试利用这些问题，而是仅仅依赖于应用程序的自我报告版本号。 | | | | | |
| **加固建议：**升级到 Apache Tomcat 7.0.57或更高版本。 | | | | | |
| High | Apache Tomcat 7.0. x < 7.0.57多重漏洞(POODLE) | CVE-2014-3512 | 7.5 | tcp | 8080 |
| **漏洞描述：**根据其自我报告的版本号，监听远程主机的 Apache Tomcat 服务在7.0.57之前是7.0.x。因此，它受到以下漏洞的影响:-d 1both.c 中存在一个内存双空闲错误，该错误与处理允许分布式拒绝服务攻击攻击的 DTLS 数据包有关。(CVE-2014-3505)-d 1 \_ both.c’中存在一个未指明的错误，该错误与处理 DTLS 握手消息有关，由于消耗了大量内存，它允许分布式拒绝服务攻击攻击。(CVE-2014-3506)-一个内存泄漏错误存在于’1both.c’中，这个错误与处理允许分布式拒绝服务攻击攻击的特制 DTLS 数据包有关。(CVE-2014-3507)-当使用各种“ X509 \_ name \_ \*”漂亮的打印函数时，“ OBJ \_ obj2txt”函数中存在错误，从而泄漏了进程堆栈数据，导致信息泄露。(CVE-2014-3508)-存在一个与“ ec 点格式扩展”处理和多线程客户机有关的错误，该客户机允许在恢复会话期间覆盖释放的内存。(CVE-2014-3509)-NULL 指针解引用错误存在于处理匿名 ECDH 密码套件和精心制作的握手消息，这些消息允许针对客户机的分布式拒绝服务攻击攻击。(CVE-2014-3510)-一个错误与处理片段化的“ ClientHello”消息有关，它允许中间的攻击者强制使用 TLS 1.0，而不管服务器和客户机支持更高的协议级别。(CVE-2014-3511)-缓冲区溢出错误存在于与处理安全远程密码协议(SRP)参数相关的‘ SRP \_ lib.c’中，这可能导致分布式拒绝服务攻击溢出或其他未指定的影响。(CVE-2014-3512)-内存泄漏问题存在于与 DTLS SRTP 扩展处理和特殊精心制作的允许分布式拒绝服务攻击攻击的握手消息有关的 d 1 \_ SRTP’中。(CVE-2014-3513)-在使用密码块链接(CBC)模式的块密码加密器加密的消息解密时，SSL 3.0处理填充字节的方式存在错误。如果中间人攻击者能够强制受害者应用程序通过新创建的 SSL 3.0连接重复发送相同的数据，那么他们只需尝试256次就可以解密密文的选定字节。这也被称为贵宾犬问题。(CVE-2014-3566)-在‘ t1 \_ lib.c’中存在一个内存泄漏问题，这个问题与允许分布式拒绝服务攻击攻击的会话票处理有关。(CVE-2014-3567)-与构建配置过程和“ no-ssl3”构建选项有关的错误，该选项允许服务器和客户端处理不安全的 SSL 3.0握手消息。(CVE-2014-3568)-一个 NULL 指针解引用错误存在于‘ t1 \_ lib.c’中，与处理安全远程密码协议(SRP) ServerHello 消息有关，它允许恶意服务器崩溃客户端，导致分布式拒绝服务攻击。(CVE-2014-5139)注意，Nessus 并没有尝试利用这些问题，而是仅仅依赖于应用程序的自我报告版本号。 | | | | | |
| **加固建议：**升级到 Apache Tomcat 7.0.57或更高版本。 | | | | | |
| High | Apache Tomcat 7.0. x < 7.0.57多重漏洞(POODLE) | CVE-2014-3513 | 7.5 | tcp | 8080 |
| **漏洞描述：**根据其自我报告的版本号，监听远程主机的 Apache Tomcat 服务在7.0.57之前是7.0.x。因此，它受到以下漏洞的影响:-d 1both.c’中存在一个内存双空闲错误，该错误与处理允许分布式拒绝服务攻击攻击的 DTLS 数据包有关。(CVE-2014-3505)-d 1 \_ both.c’中存在一个未指明的错误，该错误与处理 DTLS 握手消息有关，由于消耗了大量内存，它允许分布式拒绝服务攻击攻击。(CVE-2014-3506)-内存泄漏错误存在于’1both.c’处理特别制作的 DTLS 数据包，允许分布式拒绝服务攻击攻击。(CVE-2014-3507)-当使用各种“ X509 \_ name \_ \*”漂亮的打印函数时，“ OBJ \_ obj2txt”函数中存在一个错误，从而泄露了进程堆栈数据，导致信息泄露。(CVE-2014-3508)-存在一个与“ ec 点格式扩展”处理和多线程客户机有关的错误，该客户机允许在恢复会话期间覆盖释放的内存。(CVE-2014-3509)-NULL 指针解引用错误存在于处理匿名 ECDH 密码套件和精心制作的握手消息中，这些消息允许针对客户机的分布式拒绝服务攻击攻击。(CVE-2014-3510)-一个错误存在于处理片段化的“ ClientHello”消息中，它允许中间的攻击者强制使用 TLS 1.0，而不管服务器和客户机支持更高的协议级别。(CVE-2014-3511)-缓冲区溢出错误存在于与处理安全远程密码协议(SRP)参数相关的‘ SRP \_ lib.c’中，这可能导致分布式拒绝服务攻击溢出或其他未指定的影响。(CVE-2014-3512)-内存泄漏问题存在于与 DTLS SRTP 扩展处理和特殊制作的允许分布式拒绝服务攻击攻击的握手消息有关的 d 1 \_ SRTP’中。(CVE-2014-3513)-在使用密码块链接(CBC)模式的块密码加密器加密的消息解密时，SSL 3.0处理填充字节的方式存在错误。如果中间人攻击者能够强制受害者应用程序通过新创建的 SSL 3.0连接重复发送相同的数据，那么他们只需尝试256次就可以解密密文的选定字节。这也被称为贵宾犬问题。(CVE-2014-3566)-在‘ t1 \_ lib.c’中存在一个内存泄漏问题，这个问题与允许分布式拒绝服务攻击攻击的会话票据处理有关。(CVE-2014-3567)-与构建配置过程和“ no-ssl3”构建选项有关的错误，该选项允许服务器和客户端处理不安全的 SSL 3.0握手消息。(CVE-2014-3568)-一个 NULL 指针解引用错误存在于‘ t1 \_ lib.c’中，与处理安全远程密码协议(SRP) ServerHello 消息有关，它允许恶意服务器崩溃客户端，导致分布式拒绝服务攻击。(CVE-2014-5139)注意，Nessus 并没有尝试利用这些问题，而是仅仅依赖于应用程序的自我报告版本号。 | | | | | |
| **加固建议：**升级到 Apache Tomcat 7.0.57或更高版本。 | | | | | |
| High | Apache Tomcat 7.0. x < 7.0.57多重漏洞(POODLE) | CVE-2014-3566 | 7.5 | tcp | 8080 |
| **漏洞描述：**根据其自我报告的版本号，监听远程主机的 Apache Tomcat 服务在7.0.57之前是7.0.x。因此，它受到以下漏洞的影响:-d 1both.c 中存在一个内存双空闲错误，该错误与处理允许分布式拒绝服务攻击攻击的 DTLS 数据包有关。(CVE-2014-3505)-d 1 \_ both.c’中存在一个未指明的错误，该错误与处理 DTLS 握手消息有关，由于消耗了大量内存，它允许分布式拒绝服务攻击攻击。(CVE-2014-3506)-一个内存泄漏错误存在于’1both.c’中，这个错误与处理允许分布式拒绝服务攻击攻击的特制 DTLS 数据包有关。(CVE-2014-3507)-当使用各种“ X509 \_ name \_ \*”漂亮的打印函数时，“ OBJ \_ obj2txt”函数中存在错误，从而泄漏了进程堆栈数据，导致信息泄露。(CVE-2014-3508)-存在一个与“ ec 点格式扩展”处理和多线程客户机有关的错误，该客户机允许在恢复会话期间覆盖释放的内存。(CVE-2014-3509)-NULL 指针解引用错误存在于处理匿名 ECDH 密码套件和精心制作的握手消息，这些消息允许针对客户机的分布式拒绝服务攻击攻击。(CVE-2014-3510)-一个错误与处理片段化的“ ClientHello”消息有关，它允许中间的攻击者强制使用 TLS 1.0，而不管服务器和客户机支持更高的协议级别。(CVE-2014-3511)-缓冲区溢出错误存在于与处理安全远程密码协议(SRP)参数相关的‘ SRP \_ lib.c’中，这可能导致分布式拒绝服务攻击溢出或其他未指定的影响。(CVE-2014-3512)-内存泄漏问题存在于与 DTLS SRTP 扩展处理和特殊精心制作的允许分布式拒绝服务攻击攻击的握手消息有关的 d 1 \_ SRTP’中。(CVE-2014-3513)-在使用密码块链接(CBC)模式的块密码加密器加密的消息解密时，SSL 3.0处理填充字节的方式存在错误。如果中间人攻击者能够强制受害者应用程序通过新创建的 SSL 3.0连接重复发送相同的数据，那么他们只需尝试256次就可以解密密文的选定字节。这也被称为贵宾犬问题。(CVE-2014-3566)-在‘ t1 \_ lib.c’中存在一个内存泄漏问题，这个问题与允许分布式拒绝服务攻击攻击的会话票处理有关。(CVE-2014-3567)-与构建配置过程和“ no-ssl3”构建选项有关的错误，该选项允许服务器和客户端处理不安全的 SSL 3.0握手消息。(CVE-2014-3568)-一个 NULL 指针解引用错误存在于‘ t1 \_ lib.c’中，与处理安全远程密码协议(SRP) ServerHello 消息有关，它允许恶意服务器崩溃客户端，导致分布式拒绝服务攻击。(CVE-2014-5139)注意，Nessus 并没有尝试利用这些问题，而是仅仅依赖于应用程序的自我报告版本号。 | | | | | |
| **加固建议：**升级到 Apache Tomcat 7.0.57或更高版本。 | | | | | |
| High | Apache Tomcat 7.0. x < 7.0.57多重漏洞(POODLE) | CVE-2014-3567 | 7.5 | tcp | 8080 |
| **漏洞描述：**根据其自我报告的版本号，监听远程主机的 Apache Tomcat 服务在7.0.57之前是7.0.x。因此，它受到以下漏洞的影响:-d 1both.c 中存在一个内存双空闲错误，该错误与处理允许分布式拒绝服务攻击攻击的 DTLS 数据包有关。(CVE-2014-3505)-d 1 \_ both.c’中存在一个未指明的错误，该错误与处理 DTLS 握手消息有关，由于消耗了大量内存，它允许分布式拒绝服务攻击攻击。(CVE-2014-3506)-一个内存泄漏错误存在于’1both.c’中，这个错误与处理允许分布式拒绝服务攻击攻击的特制 DTLS 数据包有关。(CVE-2014-3507)-当使用各种“ X509 \_ name \_ \*”漂亮的打印函数时，“ OBJ \_ obj2txt”函数中存在错误，从而泄漏了进程堆栈数据，导致信息泄露。(CVE-2014-3508)-存在一个与“ ec 点格式扩展”处理和多线程客户机有关的错误，该客户机允许在恢复会话期间覆盖释放的内存。(CVE-2014-3509)-NULL 指针解引用错误存在于处理匿名 ECDH 密码套件和精心制作的握手消息，这些消息允许针对客户机的分布式拒绝服务攻击攻击。(CVE-2014-3510)-一个错误与处理片段化的“ ClientHello”消息有关，它允许中间的攻击者强制使用 TLS 1.0，而不管服务器和客户机支持更高的协议级别。(CVE-2014-3511)-缓冲区溢出错误存在于与处理安全远程密码协议(SRP)参数相关的‘ SRP \_ lib.c’中，这可能导致分布式拒绝服务攻击溢出或其他未指定的影响。(CVE-2014-3512)-内存泄漏问题存在于与 DTLS SRTP 扩展处理和特殊精心制作的允许分布式拒绝服务攻击攻击的握手消息有关的 d 1 \_ SRTP’中。(CVE-2014-3513)-在使用密码块链接(CBC)模式的块密码加密器加密的消息解密时，SSL 3.0处理填充字节的方式存在错误。如果中间人攻击者能够强制受害者应用程序通过新创建的 SSL 3.0连接重复发送相同的数据，那么他们只需尝试256次就可以解密密文的选定字节。这也被称为贵宾犬问题。(CVE-2014-3566)-在‘ t1 \_ lib.c’中存在一个内存泄漏问题，这个问题与允许分布式拒绝服务攻击攻击的会话票处理有关。(CVE-2014-3567)-与构建配置过程和“ no-ssl3”构建选项有关的错误，该选项允许服务器和客户端处理不安全的 SSL 3.0握手消息。(CVE-2014-3568)-一个 NULL 指针解引用错误存在于‘ t1 \_ lib.c’中，与处理安全远程密码协议(SRP) ServerHello 消息有关，它允许恶意服务器崩溃客户端，导致分布式拒绝服务攻击。(CVE-2014-5139)注意，Nessus 并没有尝试利用这些问题，而是仅仅依赖于应用程序的自我报告版本号。 | | | | | |
| **加固建议：**升级到 Apache Tomcat 7.0.57或更高版本。 | | | | | |
| High | Apache Tomcat 7.0. x < 7.0.57多重漏洞(POODLE) | CVE-2014-3568 | 7.5 | tcp | 8080 |
| **漏洞描述：**根据其自我报告的版本号，监听远程主机的 Apache Tomcat 服务在7.0.57之前是7.0.x。因此，它受到以下漏洞的影响:-d 1both.c 中存在一个内存双空闲错误，该错误与处理允许分布式拒绝服务攻击攻击的 DTLS 数据包有关。(CVE-2014-3505)-d 1 \_ both.c’中存在一个未指明的错误，该错误与处理 DTLS 握手消息有关，由于消耗了大量内存，它允许分布式拒绝服务攻击攻击。(CVE-2014-3506)-一个内存泄漏错误存在于’1both.c’中，这个错误与处理允许分布式拒绝服务攻击攻击的特制 DTLS 数据包有关。(CVE-2014-3507)-当使用各种“ X509 \_ name \_ \*”漂亮的打印函数时，“ OBJ \_ obj2txt”函数中存在错误，从而泄漏了进程堆栈数据，导致信息泄露。(CVE-2014-3508)-存在一个与“ ec 点格式扩展”处理和多线程客户机有关的错误，该客户机允许在恢复会话期间覆盖释放的内存。(CVE-2014-3509)-NULL 指针解引用错误存在于处理匿名 ECDH 密码套件和精心制作的握手消息，这些消息允许针对客户机的分布式拒绝服务攻击攻击。(CVE-2014-3510)-一个错误与处理片段化的“ ClientHello”消息有关，它允许中间的攻击者强制使用 TLS 1.0，而不管服务器和客户机支持更高的协议级别。(CVE-2014-3511)-缓冲区溢出错误存在于与处理安全远程密码协议(SRP)参数相关的‘ SRP \_ lib.c’中，这可能导致分布式拒绝服务攻击溢出或其他未指定的影响。(CVE-2014-3512)-内存泄漏问题存在于与 DTLS SRTP 扩展处理和特殊精心制作的允许分布式拒绝服务攻击攻击的握手消息有关的 d 1 \_ SRTP’中。(CVE-2014-3513)-在使用密码块链接(CBC)模式的块密码加密器加密的消息解密时，SSL 3.0处理填充字节的方式存在错误。如果中间人攻击者能够强制受害者应用程序通过新创建的 SSL 3.0连接重复发送相同的数据，那么他们只需尝试256次就可以解密密文的选定字节。这也被称为贵宾犬问题。(CVE-2014-3566)-在‘ t1 \_ lib.c’中存在一个内存泄漏问题，这个问题与允许分布式拒绝服务攻击攻击的会话票处理有关。(CVE-2014-3567)-与构建配置过程和“ no-ssl3”构建选项有关的错误，该选项允许服务器和客户端处理不安全的 SSL 3.0握手消息。(CVE-2014-3568)-一个 NULL 指针解引用错误存在于‘ t1 \_ lib.c’中，与处理安全远程密码协议(SRP) ServerHello 消息有关，它允许恶意服务器崩溃客户端，导致分布式拒绝服务攻击。(CVE-2014-5139)注意，Nessus 并没有尝试利用这些问题，而是仅仅依赖于应用程序的自我报告版本号。 | | | | | |
| **加固建议：**升级到 Apache Tomcat 7.0.57或更高版本。 | | | | | |
| High | Apache Tomcat 7.0. x < 7.0.57多重漏洞(POODLE) | CVE-2014-5139 | 7.5 | tcp | 8080 |
| **漏洞描述：**根据其自我报告的版本号，监听远程主机的 Apache Tomcat 服务在7.0.57之前是7.0.x。因此，它受到以下漏洞的影响:-d 1both.c 中存在一个内存双空闲错误，该错误与处理允许分布式拒绝服务攻击攻击的 DTLS 数据包有关。(CVE-2014-3505)-d 1 \_ both.c’中存在一个未指明的错误，该错误与处理 DTLS 握手消息有关，由于消耗了大量内存，它允许分布式拒绝服务攻击攻击。(CVE-2014-3506)-一个内存泄漏错误存在于’1both.c’中，这个错误与处理允许分布式拒绝服务攻击攻击的特制 DTLS 数据包有关。(CVE-2014-3507)-当使用各种“ X509 \_ name \_ \*”漂亮的打印函数时，“ OBJ \_ obj2txt”函数中存在错误，从而泄漏了进程堆栈数据，导致信息泄露。(CVE-2014-3508)-存在一个与“ ec 点格式扩展”处理和多线程客户机有关的错误，该客户机允许在恢复会话期间覆盖释放的内存。(CVE-2014-3509)-NULL 指针解引用错误存在于处理匿名 ECDH 密码套件和精心制作的握手消息，这些消息允许针对客户机的分布式拒绝服务攻击攻击。(CVE-2014-3510)-一个错误与处理片段化的“ ClientHello”消息有关，它允许中间的攻击者强制使用 TLS 1.0，而不管服务器和客户机支持更高的协议级别。(CVE-2014-3511)-缓冲区溢出错误存在于与处理安全远程密码协议(SRP)参数相关的‘ SRP \_ lib.c’中，这可能导致分布式拒绝服务攻击溢出或其他未指定的影响。(CVE-2014-3512)-内存泄漏问题存在于与 DTLS SRTP 扩展处理和特殊精心制作的允许分布式拒绝服务攻击攻击的握手消息有关的 d 1 \_ SRTP’中。(CVE-2014-3513)-在使用密码块链接(CBC)模式的块密码加密器加密的消息解密时，SSL 3.0处理填充字节的方式存在错误。如果中间人攻击者能够强制受害者应用程序通过新创建的 SSL 3.0连接重复发送相同的数据，那么他们只需尝试256次就可以解密密文的选定字节。这也被称为贵宾犬问题。(CVE-2014-3566)-在‘ t1 \_ lib.c’中存在一个内存泄漏问题，这个问题与允许分布式拒绝服务攻击攻击的会话票处理有关。(CVE-2014-3567)-与构建配置过程和“ no-ssl3”构建选项有关的错误，该选项允许服务器和客户端处理不安全的 SSL 3.0握手消息。(CVE-2014-3568)-一个 NULL 指针解引用错误存在于‘ t1 \_ lib.c’中，与处理安全远程密码协议(SRP) ServerHello 消息有关，它允许恶意服务器崩溃客户端，导致分布式拒绝服务攻击。(CVE-2014-5139)注意，Nessus 并没有尝试利用这些问题，而是仅仅依赖于应用程序的自我报告版本号。 | | | | | |
| **加固建议：**升级到 Apache Tomcat 7.0.57或更高版本。 | | | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 中危 | 名称 | CVE | CVSS | protocol | port |
| Medium | 默认文件 |  | 5.0 | tcp | 8080 |
| **漏洞描述：**在远程 Apache Tomcat 服务器上安装了默认错误页面、默认索引页面、示例 jsp 和/或示例 servlet。应该删除这些文件，因为它们可能帮助攻击者发现有关远程 Tomcat 安装或主机本身的信息。 | | | | | |
| **加固建议：**删除缺省索引页面并删除示例 JSP 和 servlet。按照 Tomcat 或 OWASP 说明替换或修改默认错误页面。 | | | | | |
| Medium | Microsoft Windows 远程桌面协议服务器中间人的弱点 | CVE-2005-1794 | 5.1 | tcp | 3389 |
| **漏洞描述：**远程桌面协议服务器(终端服务)的远程版本容易受到中间人(MiTM)攻击。在设置加密时，RDP 客户机不会努力验证服务器的标识。具有拦截 RDP 服务器流量能力的攻击者可以在不被检测到的情况下与客户机和服务器建立加密。这种性质的 MiTM 攻击允许攻击者获取传输的任何敏感信息，包括身份验证凭证。这个缺陷的存在是因为 RDP 服务器在 mstlsapi.dll 库中存储了一个硬编码的 RSA 私钥。任何能够访问这个文件(在任何 Windows 系统上)的本地用户都可以检索密钥并使用它进行此次攻击。 | | | | | |
| **加固建议：**- 如果支持，强制使用 SSL 作为此服务的传输层，或者/和-如果可用，选择“只允许从运行网络级身份验证的远程桌面计算机连接”设置。 | | | | | |
| Medium | 使用弱哈希算法签名的 SSL 证书 | CVE-2004-2761 | 5.0 | tcp | 3389 |
| **漏洞描述：**远程服务使用 SSL 证书链，该证书链使用加密弱散列算法(例如 MD2、 MD4、 MD5或 SHA1)进行签名。众所周知，这些签名算法容易受到碰撞攻击。攻击者可以利用这一点生成具有相同数字签名的另一个证书，从而允许攻击者伪装成受影响的服务。注意，这个插件报告所有用 SHA-1签署的 SSL 证书链在2017年1月1日之后过期是脆弱的。这是根据谷歌逐步取消 SHA-1加密散列算法。注意，证书链中包含在 Nessus CA 数据库(已知的 \_ CA)中。已经被忽视。 | | | | | |
| **加固建议：**联系证书颁发机构重新颁发证书。 | | | | | |
| Medium | 支持 SSL 中等强度密码组合(SWEET32) | CVE-2016-2183 | 5.0 | tcp | 3389 |
| **漏洞描述：**远程主机支持使用提供中等强度加密的 SSL 加密器。Nessus 认为中等强度的加密使用至少64位和小于112位的密钥长度，或者使用3DES 加密套件。请注意，如果攻击者位于同一物理网络上，那么绕过中等强度的加密要容易得多。 | | | | | |
| **加固建议：**重新配置受影响的应用程序，如果可能的话，避免使用中等强度的密码。 | | | | | |
| Medium | 不能信任 SSL 证书 |  | 6.4 | tcp | 3389 |
| **漏洞描述：**不能信任服务器的 x. 509证书。这种情况可能以三种不同的方式发生，其中可以破坏信任链，如下所述:-首先，服务器发送的证书链的顶端可能不是来自已知的公共证书颁发机构。这种情况可能发生在链的顶部是一个无法识别的自签名证书时，也可能发生在缺少将证书链的顶部连接到已知公共证书颁发机构的中间证书时。- 第二，证书链可能包含扫描时无效的证书。这可能发生在扫描发生在某个证书的“ notBefore”日期之前，或者发生在某个证书的“ notAfter”日期之后。- 第三，证书链可能包含与证书信息不匹配或无法验证的签名。错误签名可以通过获取带有错误签名的证书并由其签发者重新签名来修复。无法验证的签名是证书颁发者使用 Nessus 不支持或不认可的签名算法的结果。如果远程主机是生产环境中的公共主机，链路中的任何中断都会使用户更难以验证 web 服务器的真实性和身份。这使得对远程主机执行中间人攻击变得更加容易。 | | | | | |
| **加固建议：**为此服务购买或生成适当的证书。 | | | | | |
| Medium | 自签署证书 |  | 6.4 | tcp | 3389 |
| **漏洞描述：**此服务的 x. 509证书链不是由认可的证书颁发机构签名的。如果远程主机是生产环境中的公共主机，那么 SSL 的使用就无效了，因为任何人都可以针对远程主机建立中间人攻击/服务器。注意，这个插件不检查结束于非自签名证书中的证书链，而是由无法识别的证书颁发机构签名的证书链。 | | | | | |
| **加固建议：**为此服务购买或生成适当的证书。 | | | | | |
| Medium | 不需要 SMB 签名 |  | 5.0 | tcp | 445 |
| **漏洞描述：**远程 SMB 服务器上不需要签名。未经身份验证的远程攻击者可以利用这一点对 SMB 服务器进行中间人攻击。 | | | | | |
| **加固建议：**在主机配置中强制消息签名。在 Windows 上，这可以在策略设置“ Microsoft 网络服务器: 数字签名通信(总是)”中找到。在 Samba 上，这个设置称为“服务器签名”。详细信息请参阅“请参阅”链接。 | | | | | |
| Medium | 终端服务加密级别为中级或低级 |  | 4.3 | tcp | 3389 |
| **漏洞描述：**远程终端服务服务未配置为使用强加密。在此服务中使用弱加密技术可以使攻击者更容易地窃听通信并获得屏幕截图和/或击键。 | | | | | |
| **加固建议：**将 RDP 加密级别更改为: 3. High 4. FIPS Compliant | | | | | |
| Medium | 终端服务不仅使用网络级身份验证(NLA) |  | 4.3 | tcp | 3389 |
| **漏洞描述：**远程终端服务未配置为仅使用网络级身份验证(NLA)。NLA 使用凭据安全支持提供者(CredSSP)协议通过 TLS/SSL 或 Kerberos 机制执行强服务器身份验证，这些机制可以防止中间人攻击。除了改进身份验证，NLA 还通过在建立完整的 RDP 连接之前完成用户身份验证，帮助保护远程计算机免受恶意用户和软件的攻击。 | | | | | |
| **加固建议：**在远程 RDP 服务器上启用网络级身份验证(NLA)。这通常是在 Windows 的“系统”设置的“远程”选项卡上完成的。 | | | | | |
| Medium | 支持 SSL RC4密码套件(Bar Mitzvah) | CVE-2013-2566 | 4.3 | tcp | 3389 |
| **漏洞描述：**远程主机支持在一个或多个密码套件中使用 RC4。RC4密码在生成伪随机字节流方面存在缺陷，因此在字节流中引入了各种各样的小偏差，从而降低了其随机性。如果明文是重复加密的(例如 HTTP cookies) ，而攻击者能够获得许多(例如，数以千万计)密文，则攻击者可以获得明文。 | | | | | |
| **加固建议：**如果可能，重新配置受影响的应用程序，以避免使用 RC4密码。考虑在浏览器和 web 服务器支持的条件下使用带有 AES-GCM 套件的 TLS 1.2。 | | | | | |
| Medium | 支持 SSL RC4密码套件(Bar Mitzvah) | CVE-2015-2808 | 4.3 | tcp | 3389 |
| **漏洞描述：**远程主机支持在一个或多个密码套件中使用 RC4。RC4密码在生成伪随机字节流方面存在缺陷，因此在字节流中引入了各种各样的小偏差，从而降低了其随机性。如果明文是重复加密的(例如 HTTP cookies) ，而攻击者能够获得许多(例如，数以千万计)密文，则攻击者可以获得明文。 | | | | | |
| **加固建议：**如果可能，重新配置受影响的应用程序，以避免使用 RC4密码。考虑在浏览器和 web 服务器支持的条件下使用带有 AES-GCM 套件的 TLS 1.2。 | | | | | |
| Medium | Apache Tomcat 7.0. x < 7.0.60多个漏洞(FREAK) | CVE-2014-3569 | 6.8 | tcp | 8080 |
| **漏洞描述：**根据其自我报告的版本号，监听远程主机的 Apache Tomcat 服务在7.0.60之前是7.0.x。因此，它受到以下漏洞的影响:-当 SSLv3选项未启用且接收到 SSLv3 ClientHello 时，存在一个 NULL 指针取消引用缺陷。这使得远程攻击者可以使用意外的握手来崩溃守护进程，从而导致分布式拒绝服务攻击攻击。(CVE-2014-3569)-BIGNUM 平方(BN \_ sqr)实现没有正确计算 BIGNUM 值的平方。这使得远程攻击者可以击败加密保护机制。(CVE-2014-3570)-当处理 dtls1 \_ get \_ record ()消息时，存在一个 NULL 指针解引用缺陷。一个远程攻击者，使用一个特制的 DTLS 消息，可以导致一个分布式拒绝服务攻击。(CVE-2014-3571)-当使用没有 ServerKeyExchange 消息的 ECDSA 证书时，ECDH 握手存在缺陷。这允许远程攻击者触发来自密码套件的前向保密丢失。(CVE-2014-3572)-在接受证书签名算法和签名编码的非 der 变体时存在缺陷，原因是没有强制执行已签名和未签名部分之间的匹配。远程攻击者通过在证书的未签名部分包含精心制作的数据，可以绕过基于指纹的证书黑名单保护机制。(CVE-2014-8275)-一种安全特性绕过漏洞，称为 FREAK (对 RSA-EXPORT 密钥的因式分解攻击) ，由于支持密钥小于或等于512位的弱 EXPORT \_ rsa 密码套件而存在。中间人攻击者可以降低 SSL/TLS 连接的等级，使用 EXPORT \_ rsa 密码组合，该组合可以在短时间内分解，允许攻击者拦截和解密流量。(CVE-2015-0204)-在没有认证验证消息的情况下接受用于客户端身份验证的 DH 证书存在缺陷。这允许远程攻击者在没有私钥的情况下对服务进行身份验证。(CVE-2015-0205)-当处理包含相同数字序列但下一个历元的 DTLS 记录的饱和时，dtls1\_buffer \_ record ()发生内存泄漏。这使得远程攻击者可以引发分布式拒绝服务攻击攻击。(CVE-2015-0206)-由于在导入过程中对格式错误的 EC 私钥文件处理不当，d2i \_ ecprivatedkey ()函数中存在一个 use-after-free 条件。远程攻击者可以利用这一点取消引用或释放已释放的内存，从而导致分布式拒绝服务攻击或其他未指定的影响。(CVE-2015-0209)-ASN1 \_ type \_ cmp ()函数中存在无效的读缺陷，原因是布尔类型比较执行不当。远程攻击者可以利用这一点，通过一个精心设计的 x. 509证书到一个使用证书验证特性的端点，导致一个无效的读操作，造成一个分布式拒绝服务攻击。(CVE-2015-0286)-ASN1 \_ item \_ ex \_ d2i ()函数中存在一个缺陷，原因是在 ASN. 1解析中重用结构时未能重新初始化“ CHOICE”和“ ADB”数据结构。这允许远程攻击者造成无效的写操作和内存损坏，从而导致分布式拒绝服务攻击攻击。(CVE-2015-0287)-由于证书密钥处理不当，X509 \_ to \_ X509 \_ req ()函数中存在空指针解引用缺陷。这允许远程攻击者通过一个精心设计的 x. 509证书，引发一个分布式拒绝服务攻击攻击。(CVE-2015-0288)-由于错误处理丢失的外部 ContentInfo，PKCS # 7解析代码中存在 NULL 指针解引用缺陷。这允许远程攻击者使用处理任意 PKCS # 7数据的应用程序，并使用 ASN. 1编码提供格式不正确的数据，从而导致分布式拒绝服务攻击攻击。(CVE-2015-0289)-由于 SSLv2的实现不当，同时支持 SSLv2和启用导出密码套件的服务器中存在一个缺陷。远程攻击者可以利用这一点，通过一个精心设计的 CLIENT-MASTER-KEY 消息，引发分布式拒绝服务攻击攻击。(CVE-2015-0293)注意，Nessus 并没有尝试利用这些问题，而是仅仅依赖于应用程序的自我报告版本号。 | | | | | |
| **加固建议：**升级到 Apache Tomcat 7.0.60或更高版本。 | | | | | |
| Medium | Apache Tomcat 7.0. x < 7.0.60多个漏洞(FREAK) | CVE-2014-3570 | 6.8 | tcp | 8080 |
| **漏洞描述：**根据其自我报告的版本号，监听远程主机的 Apache Tomcat 服务在7.0.60之前是7.0.x。因此，它受到以下漏洞的影响:-当 SSLv3选项未启用且接收到 SSLv3 ClientHello 时，存在 NULL 指针解引用缺陷。这使得远程攻击者可以使用意外的握手来崩溃守护进程，从而导致分布式拒绝服务攻击攻击。(CVE-2014-3569)-BIGNUM 平方(BN \_ sqr)实现没有正确计算 BIGNUM 值的平方。这使得远程攻击者可以击败加密保护机制。(CVE-2014-3570)-在处理 DTLS 消息时，使用 dtls1 \_ get \_ record ()存在一个 NULL 指针解引用缺陷。一个远程攻击者，使用一个特制的 DTLS 消息，可以导致一个分布式拒绝服务攻击。(CVE-2014-3571)-当使用没有 ServerKeyExchange 消息的 ECDSA 证书时，ECDH 握手存在缺陷。这允许远程攻击者触发来自密码套件的前向保密丢失。(CVE-2014-3572)-在接受证书签名算法和签名编码的非 der 变体时存在缺陷，原因是没有强制执行已签名和未签名部分之间的匹配。远程攻击者通过在证书的未签名部分包含精心制作的数据，可以绕过基于指纹的证书黑名单保护机制。(CVE-2014-8275)-一个安全特性绕过漏洞，被称为 FREAK (对 RSA-EXPORT 密钥的因式分解攻击) ，由于支持密钥小于或等于512位的弱 EXPORT \_ rsa 密码套件而存在。中间人攻击者可以降低 SSL/TLS 连接的等级，使用 EXPORT \_ rsa 密码组合，该组合可以在短时间内分解，允许攻击者拦截和解密流量。(CVE-2015-0204)-在没有认证验证消息的情况下接受客户端身份验证的 DH 证书存在缺陷。这允许远程攻击者在没有私钥的情况下对服务进行身份验证。(CVE-2015-0205)-当处理包含相同数字序列但下一个历元的 DTLS 记录的饱和时，dtls1\_buffer \_ record ()发生内存泄漏。这使得远程攻击者可以引发分布式拒绝服务攻击攻击。(CVE-2015-0206)-由于在导入过程中对格式错误的 EC 私钥文件处理不当，d2i \_ ecprivatedkey ()函数中存在一个 use-after-free 条件。远程攻击者可以利用这一点取消引用或释放已释放的内存，从而导致分布式拒绝服务攻击或其他未指定的影响。(CVE-2015-0209)-ASN1 \_ type \_ cmp ()函数中存在无效的读缺陷，原因是布尔类型比较执行不当。远程攻击者可以利用这一点，通过一个精心设计的 x. 509证书到一个使用证书验证特性的端点，导致一个无效的读操作，造成一个分布式拒绝服务攻击。(CVE-2015-0286)-ASN1 \_ item \_ ex \_ d2i ()函数中存在一个缺陷，原因是在 ASN. 1解析中重用结构时未能重新初始化“ CHOICE”和“ ADB”数据结构。这允许远程攻击者造成无效的写操作和内存损坏，从而导致分布式拒绝服务攻击攻击。(CVE-2015-0287)-由于证书密钥处理不当，X509 \_ to \_ X509 \_ req ()函数中存在空指针解引用缺陷。这允许远程攻击者通过一个精心设计的 x. 509证书，引发一个分布式拒绝服务攻击攻击。(CVE-2015-0288)-由于错误处理丢失的外部 ContentInfo，PKCS # 7解析代码中存在 NULL 指针解引用缺陷。这允许远程攻击者使用处理任意 PKCS # 7数据的应用程序，并使用 ASN. 1编码提供格式不正确的数据，从而导致分布式拒绝服务攻击攻击。(CVE-2015-0289)-由于 SSLv2的实现不当，同时支持 SSLv2和启用导出密码套件的服务器中存在一个缺陷。远程攻击者可以利用这一点，通过一个精心设计的 CLIENT-MASTER-KEY 消息，引发分布式拒绝服务攻击攻击。(CVE-2015-0293)注意，Nessus 并没有尝试利用这些问题，而是仅仅依赖于应用程序的自我报告版本号。 | | | | | |
| **加固建议：**升级到 Apache Tomcat 7.0.60或更高版本。 | | | | | |
| Medium | Apache Tomcat 7.0. x < 7.0.60多个漏洞(FREAK) | CVE-2014-3571 | 6.8 | tcp | 8080 |
| **漏洞描述：**根据其自我报告的版本号，监听远程主机的 Apache Tomcat 服务在7.0.60之前是7.0.x。因此，它受到以下漏洞的影响:-当 SSLv3选项未启用且接收到 SSLv3 ClientHello 时，存在一个 NULL 指针取消引用缺陷。这使得远程攻击者可以使用意外的握手来崩溃守护进程，从而导致分布式拒绝服务攻击攻击。(CVE-2014-3569)-BIGNUM 平方(BN \_ sqr)实现没有正确计算 BIGNUM 值的平方。这使得远程攻击者可以击败加密保护机制。(CVE-2014-3570)-当处理 dtls1 \_ get \_ record ()消息时，存在一个 NULL 指针解引用缺陷。一个远程攻击者，使用一个特制的 DTLS 消息，可以导致一个分布式拒绝服务攻击。(CVE-2014-3571)-当使用没有 ServerKeyExchange 消息的 ECDSA 证书时，ECDH 握手存在缺陷。这允许远程攻击者触发来自密码套件的前向保密丢失。(CVE-2014-3572)-在接受证书签名算法和签名编码的非 der 变体时存在缺陷，原因是没有强制执行已签名和未签名部分之间的匹配。远程攻击者通过在证书的未签名部分包含精心制作的数据，可以绕过基于指纹的证书黑名单保护机制。(CVE-2014-8275)-一种安全特性绕过漏洞，称为 FREAK (对 RSA-EXPORT 密钥的因式分解攻击) ，由于支持密钥小于或等于512位的弱 EXPORT \_ rsa 密码套件而存在。中间人攻击者可以降低 SSL/TLS 连接的等级，使用 EXPORT \_ rsa 密码组合，该组合可以在短时间内分解，允许攻击者拦截和解密流量。(CVE-2015-0204)-在没有认证验证消息的情况下接受用于客户端身份验证的 DH 证书存在缺陷。这允许远程攻击者在没有私钥的情况下对服务进行身份验证。(CVE-2015-0205)-当处理包含相同数字序列但下一个历元的 DTLS 记录的饱和时，dtls1\_buffer \_ record ()发生内存泄漏。这使得远程攻击者可以引发分布式拒绝服务攻击攻击。(CVE-2015-0206)-由于在导入过程中对格式错误的 EC 私钥文件处理不当，d2i \_ ecprivatedkey ()函数中存在一个 use-after-free 条件。远程攻击者可以利用这一点取消引用或释放已释放的内存，从而导致分布式拒绝服务攻击或其他未指定的影响。(CVE-2015-0209)-ASN1 \_ type \_ cmp ()函数中存在无效的读缺陷，原因是布尔类型比较执行不当。远程攻击者可以利用这一点，通过一个精心设计的 x. 509证书到一个使用证书验证特性的端点，导致一个无效的读操作，造成一个分布式拒绝服务攻击。(CVE-2015-0286)-ASN1 \_ item \_ ex \_ d2i ()函数中存在一个缺陷，原因是在 ASN. 1解析中重用结构时未能重新初始化“ CHOICE”和“ ADB”数据结构。这允许远程攻击者造成无效的写操作和内存损坏，从而导致分布式拒绝服务攻击攻击。(CVE-2015-0287)-由于证书密钥处理不当，X509 \_ to \_ X509 \_ req ()函数中存在空指针解引用缺陷。这允许远程攻击者通过一个精心设计的 x. 509证书，引发一个分布式拒绝服务攻击攻击。(CVE-2015-0288)-由于错误处理丢失的外部 ContentInfo，PKCS # 7解析代码中存在 NULL 指针解引用缺陷。这允许远程攻击者使用处理任意 PKCS # 7数据的应用程序，并使用 ASN. 1编码提供格式不正确的数据，从而导致分布式拒绝服务攻击攻击。(CVE-2015-0289)-由于 SSLv2的实现不当，同时支持 SSLv2和启用导出密码套件的服务器中存在一个缺陷。远程攻击者可以利用这一点，通过一个精心设计的 CLIENT-MASTER-KEY 消息，引发分布式拒绝服务攻击攻击。(CVE-2015-0293)注意，Nessus 并没有尝试利用这些问题，而是仅仅依赖于应用程序的自我报告版本号。 | | | | | |
| **加固建议：**升级到 Apache Tomcat 7.0.60或更高版本。 | | | | | |
| Medium | Apache Tomcat 7.0. x < 7.0.60多个漏洞(FREAK) | CVE-2014-3572 | 6.8 | tcp | 8080 |
| **漏洞描述：**根据其自我报告的版本号，监听远程主机的 Apache Tomcat 服务在7.0.60之前是7.0.x。因此，它受到以下漏洞的影响:-当 SSLv3选项未启用且接收到 SSLv3 ClientHello 时，存在一个 NULL 指针取消引用缺陷。这使得远程攻击者可以使用意外的握手来崩溃守护进程，从而导致分布式拒绝服务攻击攻击。(CVE-2014-3569)-BIGNUM 平方(BN \_ sqr)实现没有正确计算 BIGNUM 值的平方。这使得远程攻击者可以击败加密保护机制。(CVE-2014-3570)-当处理 dtls1 \_ get \_ record ()消息时，存在一个 NULL 指针解引用缺陷。一个远程攻击者，使用一个特制的 DTLS 消息，可以导致一个分布式拒绝服务攻击。(CVE-2014-3571)-当使用没有 ServerKeyExchange 消息的 ECDSA 证书时，ECDH 握手存在缺陷。这允许远程攻击者触发来自密码套件的前向保密丢失。(CVE-2014-3572)-在接受证书签名算法和签名编码的非 der 变体时存在缺陷，原因是没有强制执行已签名和未签名部分之间的匹配。远程攻击者通过在证书的未签名部分包含精心制作的数据，可以绕过基于指纹的证书黑名单保护机制。(CVE-2014-8275)-一种安全特性绕过漏洞，称为 FREAK (对 RSA-EXPORT 密钥的因式分解攻击) ，由于支持密钥小于或等于512位的弱 EXPORT \_ rsa 密码套件而存在。中间人攻击者可以降低 SSL/TLS 连接的等级，使用 EXPORT \_ rsa 密码组合，该组合可以在短时间内分解，允许攻击者拦截和解密流量。(CVE-2015-0204)-在没有认证验证消息的情况下接受用于客户端身份验证的 DH 证书存在缺陷。这允许远程攻击者在没有私钥的情况下对服务进行身份验证。(CVE-2015-0205)-当处理包含相同数字序列但下一个历元的 DTLS 记录的饱和时，dtls1\_buffer \_ record ()发生内存泄漏。这使得远程攻击者可以引发分布式拒绝服务攻击攻击。(CVE-2015-0206)-由于在导入过程中对格式错误的 EC 私钥文件处理不当，d2i \_ ecprivatedkey ()函数中存在一个 use-after-free 条件。远程攻击者可以利用这一点取消引用或释放已释放的内存，从而导致分布式拒绝服务攻击或其他未指定的影响。(CVE-2015-0209)-ASN1 \_ type \_ cmp ()函数中存在无效的读缺陷，原因是布尔类型比较执行不当。远程攻击者可以利用这一点，通过一个精心设计的 x. 509证书到一个使用证书验证特性的端点，导致一个无效的读操作，造成一个分布式拒绝服务攻击。(CVE-2015-0286)-ASN1 \_ item \_ ex \_ d2i ()函数中存在一个缺陷，原因是在 ASN. 1解析中重用结构时未能重新初始化“ CHOICE”和“ ADB”数据结构。这允许远程攻击者造成无效的写操作和内存损坏，从而导致分布式拒绝服务攻击攻击。(CVE-2015-0287)-由于证书密钥处理不当，X509 \_ to \_ X509 \_ req ()函数中存在空指针解引用缺陷。这允许远程攻击者通过一个精心设计的 x. 509证书，引发一个分布式拒绝服务攻击攻击。(CVE-2015-0288)-由于错误处理丢失的外部 ContentInfo，PKCS # 7解析代码中存在 NULL 指针解引用缺陷。这允许远程攻击者使用处理任意 PKCS # 7数据的应用程序，并使用 ASN. 1编码提供格式不正确的数据，从而导致分布式拒绝服务攻击攻击。(CVE-2015-0289)-由于 SSLv2的实现不当，同时支持 SSLv2和启用导出密码套件的服务器中存在一个缺陷。远程攻击者可以利用这一点，通过一个精心设计的 CLIENT-MASTER-KEY 消息，引发分布式拒绝服务攻击攻击。(CVE-2015-0293)注意，Nessus 并没有尝试利用这些问题，而是仅仅依赖于应用程序的自我报告版本号。 | | | | | |
| **加固建议：**升级到 Apache Tomcat 7.0.60或更高版本。 | | | | | |
| Medium | Apache Tomcat 7.0. x < 7.0.60多个漏洞(FREAK) | CVE-2014-8275 | 6.8 | tcp | 8080 |
| **漏洞描述：**根据其自我报告的版本号，监听远程主机的 Apache Tomcat 服务在7.0.60之前是7.0.x。因此，它受到以下漏洞的影响:-当 SSLv3选项未启用且接收到 SSLv3 ClientHello 时，存在一个 NULL 指针取消引用缺陷。这使得远程攻击者可以使用意外的握手来崩溃守护进程，从而导致分布式拒绝服务攻击攻击。(CVE-2014-3569)-BIGNUM 平方(BN \_ sqr)实现没有正确计算 BIGNUM 值的平方。这使得远程攻击者可以击败加密保护机制。(CVE-2014-3570)-当处理 dtls1 \_ get \_ record ()消息时，存在一个 NULL 指针解引用缺陷。一个远程攻击者，使用一个特制的 DTLS 消息，可以导致一个分布式拒绝服务攻击。(CVE-2014-3571)-当使用没有 ServerKeyExchange 消息的 ECDSA 证书时，ECDH 握手存在缺陷。这允许远程攻击者触发来自密码套件的前向保密丢失。(CVE-2014-3572)-在接受证书签名算法和签名编码的非 der 变体时存在缺陷，原因是没有强制执行已签名和未签名部分之间的匹配。远程攻击者通过在证书的未签名部分包含精心制作的数据，可以绕过基于指纹的证书黑名单保护机制。(CVE-2014-8275)-一种安全特性绕过漏洞，称为 FREAK (对 RSA-EXPORT 密钥的因式分解攻击) ，由于支持密钥小于或等于512位的弱 EXPORT \_ rsa 密码套件而存在。中间人攻击者可以降低 SSL/TLS 连接的等级，使用 EXPORT \_ rsa 密码组合，该组合可以在短时间内分解，允许攻击者拦截和解密流量。(CVE-2015-0204)-在没有认证验证消息的情况下接受用于客户端身份验证的 DH 证书存在缺陷。这允许远程攻击者在没有私钥的情况下对服务进行身份验证。(CVE-2015-0205)-当处理包含相同数字序列但下一个历元的 DTLS 记录的饱和时，dtls1\_buffer \_ record ()发生内存泄漏。这使得远程攻击者可以引发分布式拒绝服务攻击攻击。(CVE-2015-0206)-由于在导入过程中对格式错误的 EC 私钥文件处理不当，d2i \_ ecprivatedkey ()函数中存在一个 use-after-free 条件。远程攻击者可以利用这一点取消引用或释放已释放的内存，从而导致分布式拒绝服务攻击或其他未指定的影响。(CVE-2015-0209)-ASN1 \_ type \_ cmp ()函数中存在无效的读缺陷，原因是布尔类型比较执行不当。远程攻击者可以利用这一点，通过一个精心设计的 x. 509证书到一个使用证书验证特性的端点，导致一个无效的读操作，造成一个分布式拒绝服务攻击。(CVE-2015-0286)-ASN1 \_ item \_ ex \_ d2i ()函数中存在一个缺陷，原因是在 ASN. 1解析中重用结构时未能重新初始化“ CHOICE”和“ ADB”数据结构。这允许远程攻击者造成无效的写操作和内存损坏，从而导致分布式拒绝服务攻击攻击。(CVE-2015-0287)-由于证书密钥处理不当，X509 \_ to \_ X509 \_ req ()函数中存在空指针解引用缺陷。这允许远程攻击者通过一个精心设计的 x. 509证书，引发一个分布式拒绝服务攻击攻击。(CVE-2015-0288)-由于错误处理丢失的外部 ContentInfo，PKCS # 7解析代码中存在 NULL 指针解引用缺陷。这允许远程攻击者使用处理任意 PKCS # 7数据的应用程序，并使用 ASN. 1编码提供格式不正确的数据，从而导致分布式拒绝服务攻击攻击。(CVE-2015-0289)-由于 SSLv2的实现不当，同时支持 SSLv2和启用导出密码套件的服务器中存在一个缺陷。远程攻击者可以利用这一点，通过一个精心设计的 CLIENT-MASTER-KEY 消息，引发分布式拒绝服务攻击攻击。(CVE-2015-0293)注意，Nessus 并没有尝试利用这些问题，而是仅仅依赖于应用程序的自我报告版本号。 | | | | | |
| **加固建议：**升级到 Apache Tomcat 7.0.60或更高版本。 | | | | | |
| Medium | Apache Tomcat 7.0. x < 7.0.60多个漏洞(FREAK) | CVE-2015-0204 | 6.8 | tcp | 8080 |
| **漏洞描述：**根据其自我报告的版本号，监听远程主机的 Apache Tomcat 服务在7.0.60之前是7.0.x。因此，它受到以下漏洞的影响:-当 SSLv3选项未启用且接收到 SSLv3 ClientHello 时，存在一个 NULL 指针取消引用缺陷。这使得远程攻击者可以使用意外的握手来崩溃守护进程，从而导致分布式拒绝服务攻击攻击。(CVE-2014-3569)-BIGNUM 平方(BN \_ sqr)实现没有正确计算 BIGNUM 值的平方。这使得远程攻击者可以击败加密保护机制。(CVE-2014-3570)-当处理 dtls1 \_ get \_ record ()消息时，存在一个 NULL 指针解引用缺陷。一个远程攻击者，使用一个特制的 DTLS 消息，可以导致一个分布式拒绝服务攻击。(CVE-2014-3571)-当使用没有 ServerKeyExchange 消息的 ECDSA 证书时，ECDH 握手存在缺陷。这允许远程攻击者触发来自密码套件的前向保密丢失。(CVE-2014-3572)-在接受证书签名算法和签名编码的非 der 变体时存在缺陷，原因是没有强制执行已签名和未签名部分之间的匹配。远程攻击者通过在证书的未签名部分包含精心制作的数据，可以绕过基于指纹的证书黑名单保护机制。(CVE-2014-8275)-一种安全特性绕过漏洞，称为 FREAK (对 RSA-EXPORT 密钥的因式分解攻击) ，由于支持密钥小于或等于512位的弱 EXPORT \_ rsa 密码套件而存在。中间人攻击者可以降低 SSL/TLS 连接的等级，使用 EXPORT \_ rsa 密码组合，该组合可以在短时间内分解，允许攻击者拦截和解密流量。(CVE-2015-0204)-在没有认证验证消息的情况下接受用于客户端身份验证的 DH 证书存在缺陷。这允许远程攻击者在没有私钥的情况下对服务进行身份验证。(CVE-2015-0205)-当处理包含相同数字序列但下一个历元的 DTLS 记录的饱和时，dtls1\_buffer \_ record ()发生内存泄漏。这使得远程攻击者可以引发分布式拒绝服务攻击攻击。(CVE-2015-0206)-由于在导入过程中对格式错误的 EC 私钥文件处理不当，d2i \_ ecprivatedkey ()函数中存在一个 use-after-free 条件。远程攻击者可以利用这一点取消引用或释放已释放的内存，从而导致分布式拒绝服务攻击或其他未指定的影响。(CVE-2015-0209)-ASN1 \_ type \_ cmp ()函数中存在无效的读缺陷，原因是布尔类型比较执行不当。远程攻击者可以利用这一点，通过一个精心设计的 x. 509证书到一个使用证书验证特性的端点，导致一个无效的读操作，造成一个分布式拒绝服务攻击。(CVE-2015-0286)-ASN1 \_ item \_ ex \_ d2i ()函数中存在一个缺陷，原因是在 ASN. 1解析中重用结构时未能重新初始化“ CHOICE”和“ ADB”数据结构。这允许远程攻击者造成无效的写操作和内存损坏，从而导致分布式拒绝服务攻击攻击。(CVE-2015-0287)-由于证书密钥处理不当，X509 \_ to \_ X509 \_ req ()函数中存在空指针解引用缺陷。这允许远程攻击者通过一个精心设计的 x. 509证书，引发一个分布式拒绝服务攻击攻击。(CVE-2015-0288)-由于错误处理丢失的外部 ContentInfo，PKCS # 7解析代码中存在 NULL 指针解引用缺陷。这允许远程攻击者使用处理任意 PKCS # 7数据的应用程序，并使用 ASN. 1编码提供格式不正确的数据，从而导致分布式拒绝服务攻击攻击。(CVE-2015-0289)-由于 SSLv2的实现不当，同时支持 SSLv2和启用导出密码套件的服务器中存在一个缺陷。远程攻击者可以利用这一点，通过一个精心设计的 CLIENT-MASTER-KEY 消息，引发分布式拒绝服务攻击攻击。(CVE-2015-0293)注意，Nessus 并没有尝试利用这些问题，而是仅仅依赖于应用程序的自我报告版本号。 | | | | | |
| **加固建议：**升级到 Apache Tomcat 7.0.60或更高版本。 | | | | | |
| Medium | Apache Tomcat 7.0. x < 7.0.60多个漏洞(FREAK) | CVE-2015-0205 | 6.8 | tcp | 8080 |
| **漏洞描述：**根据其自我报告的版本号，监听远程主机的 Apache Tomcat 服务在7.0.60之前是7.0.x。因此，它受到以下漏洞的影响:-当 SSLv3选项未启用且接收到 SSLv3 ClientHello 时，存在一个 NULL 指针取消引用缺陷。这使得远程攻击者可以使用意外的握手来崩溃守护进程，从而导致分布式拒绝服务攻击攻击。(CVE-2014-3569)-BIGNUM 平方(BN \_ sqr)实现没有正确计算 BIGNUM 值的平方。这使得远程攻击者可以击败加密保护机制。(CVE-2014-3570)-当处理 dtls1 \_ get \_ record ()消息时，存在一个 NULL 指针解引用缺陷。一个远程攻击者，使用一个特制的 DTLS 消息，可以导致一个分布式拒绝服务攻击。(CVE-2014-3571)-当使用没有 ServerKeyExchange 消息的 ECDSA 证书时，ECDH 握手存在缺陷。这允许远程攻击者触发来自密码套件的前向保密丢失。(CVE-2014-3572)-在接受证书签名算法和签名编码的非 der 变体时存在缺陷，原因是没有强制执行已签名和未签名部分之间的匹配。远程攻击者通过在证书的未签名部分包含精心制作的数据，可以绕过基于指纹的证书黑名单保护机制。(CVE-2014-8275)-一种安全特性绕过漏洞，称为 FREAK (对 RSA-EXPORT 密钥的因式分解攻击) ，由于支持密钥小于或等于512位的弱 EXPORT \_ rsa 密码套件而存在。中间人攻击者可以降低 SSL/TLS 连接的等级，使用 EXPORT \_ rsa 密码组合，该组合可以在短时间内分解，允许攻击者拦截和解密流量。(CVE-2015-0204)-在没有认证验证消息的情况下接受用于客户端身份验证的 DH 证书存在缺陷。这允许远程攻击者在没有私钥的情况下对服务进行身份验证。(CVE-2015-0205)-当处理包含相同数字序列但下一个历元的 DTLS 记录的饱和时，dtls1\_buffer \_ record ()发生内存泄漏。这使得远程攻击者可以引发分布式拒绝服务攻击攻击。(CVE-2015-0206)-由于在导入过程中对格式错误的 EC 私钥文件处理不当，d2i \_ ecprivatedkey ()函数中存在一个 use-after-free 条件。远程攻击者可以利用这一点取消引用或释放已释放的内存，从而导致分布式拒绝服务攻击或其他未指定的影响。(CVE-2015-0209)-ASN1 \_ type \_ cmp ()函数中存在无效的读缺陷，原因是布尔类型比较执行不当。远程攻击者可以利用这一点，通过一个精心设计的 x. 509证书到一个使用证书验证特性的端点，导致一个无效的读操作，造成一个分布式拒绝服务攻击。(CVE-2015-0286)-ASN1 \_ item \_ ex \_ d2i ()函数中存在一个缺陷，原因是在 ASN. 1解析中重用结构时未能重新初始化“ CHOICE”和“ ADB”数据结构。这允许远程攻击者造成无效的写操作和内存损坏，从而导致分布式拒绝服务攻击攻击。(CVE-2015-0287)-由于证书密钥处理不当，X509 \_ to \_ X509 \_ req ()函数中存在空指针解引用缺陷。这允许远程攻击者通过一个精心设计的 x. 509证书，引发一个分布式拒绝服务攻击攻击。(CVE-2015-0288)-由于错误处理丢失的外部 ContentInfo，PKCS # 7解析代码中存在 NULL 指针解引用缺陷。这允许远程攻击者使用处理任意 PKCS # 7数据的应用程序，并使用 ASN. 1编码提供格式不正确的数据，从而导致分布式拒绝服务攻击攻击。(CVE-2015-0289)-由于 SSLv2的实现不当，同时支持 SSLv2和启用导出密码套件的服务器中存在一个缺陷。远程攻击者可以利用这一点，通过一个精心设计的 CLIENT-MASTER-KEY 消息，引发分布式拒绝服务攻击攻击。(CVE-2015-0293)注意，Nessus 并没有尝试利用这些问题，而是仅仅依赖于应用程序的自我报告版本号。 | | | | | |
| **加固建议：**升级到 Apache Tomcat 7.0.60或更高版本。 | | | | | |
| Medium | Apache Tomcat 7.0. x < 7.0.60多个漏洞(FREAK) | CVE-2015-0206 | 6.8 | tcp | 8080 |
| **漏洞描述：**根据其自我报告的版本号，监听远程主机的 Apache Tomcat 服务在7.0.60之前是7.0.x。因此，它受到以下漏洞的影响:-当 SSLv3选项未启用且接收到 SSLv3 ClientHello 时，存在一个 NULL 指针取消引用缺陷。这使得远程攻击者可以使用意外的握手来崩溃守护进程，从而导致分布式拒绝服务攻击攻击。(CVE-2014-3569)-BIGNUM 平方(BN \_ sqr)实现没有正确计算 BIGNUM 值的平方。这使得远程攻击者可以击败加密保护机制。(CVE-2014-3570)-当处理 dtls1 \_ get \_ record ()消息时，存在一个 NULL 指针解引用缺陷。一个远程攻击者，使用一个特制的 DTLS 消息，可以导致一个分布式拒绝服务攻击。(CVE-2014-3571)-当使用没有 ServerKeyExchange 消息的 ECDSA 证书时，ECDH 握手存在缺陷。这允许远程攻击者触发来自密码套件的前向保密丢失。(CVE-2014-3572)-在接受证书签名算法和签名编码的非 der 变体时存在缺陷，原因是没有强制执行已签名和未签名部分之间的匹配。远程攻击者通过在证书的未签名部分包含精心制作的数据，可以绕过基于指纹的证书黑名单保护机制。(CVE-2014-8275)-一种安全特性绕过漏洞，称为 FREAK (对 RSA-EXPORT 密钥的因式分解攻击) ，由于支持密钥小于或等于512位的弱 EXPORT \_ rsa 密码套件而存在。中间人攻击者可以降低 SSL/TLS 连接的等级，使用 EXPORT \_ rsa 密码组合，该组合可以在短时间内分解，允许攻击者拦截和解密流量。(CVE-2015-0204)-在没有认证验证消息的情况下接受用于客户端身份验证的 DH 证书存在缺陷。这允许远程攻击者在没有私钥的情况下对服务进行身份验证。(CVE-2015-0205)-当处理包含相同数字序列但下一个历元的 DTLS 记录的饱和时，dtls1\_buffer \_ record ()发生内存泄漏。这使得远程攻击者可以引发分布式拒绝服务攻击攻击。(CVE-2015-0206)-由于在导入过程中对格式错误的 EC 私钥文件处理不当，d2i \_ ecprivatedkey ()函数中存在一个 use-after-free 条件。远程攻击者可以利用这一点取消引用或释放已释放的内存，从而导致分布式拒绝服务攻击或其他未指定的影响。(CVE-2015-0209)-ASN1 \_ type \_ cmp ()函数中存在无效的读缺陷，原因是布尔类型比较执行不当。远程攻击者可以利用这一点，通过一个精心设计的 x. 509证书到一个使用证书验证特性的端点，导致一个无效的读操作，造成一个分布式拒绝服务攻击。(CVE-2015-0286)-ASN1 \_ item \_ ex \_ d2i ()函数中存在一个缺陷，原因是在 ASN. 1解析中重用结构时未能重新初始化“ CHOICE”和“ ADB”数据结构。这允许远程攻击者造成无效的写操作和内存损坏，从而导致分布式拒绝服务攻击攻击。(CVE-2015-0287)-由于证书密钥处理不当，X509 \_ to \_ X509 \_ req ()函数中存在空指针解引用缺陷。这允许远程攻击者通过一个精心设计的 x. 509证书，引发一个分布式拒绝服务攻击攻击。(CVE-2015-0288)-由于错误处理丢失的外部 ContentInfo，PKCS # 7解析代码中存在 NULL 指针解引用缺陷。这允许远程攻击者使用处理任意 PKCS # 7数据的应用程序，并使用 ASN. 1编码提供格式不正确的数据，从而导致分布式拒绝服务攻击攻击。(CVE-2015-0289)-由于 SSLv2的实现不当，同时支持 SSLv2和启用导出密码套件的服务器中存在一个缺陷。远程攻击者可以利用这一点，通过一个精心设计的 CLIENT-MASTER-KEY 消息，引发分布式拒绝服务攻击攻击。(CVE-2015-0293)注意，Nessus 并没有尝试利用这些问题，而是仅仅依赖于应用程序的自我报告版本号。 | | | | | |
| **加固建议：**升级到 Apache Tomcat 7.0.60或更高版本。 | | | | | |
| Medium | Apache Tomcat 7.0. x < 7.0.60多个漏洞(FREAK) | CVE-2015-0209 | 6.8 | tcp | 8080 |
| **漏洞描述：**根据其自我报告的版本号，监听远程主机的 Apache Tomcat 服务在7.0.60之前是7.0.x。因此，它受到以下漏洞的影响:-当 SSLv3选项未启用且接收到 SSLv3 ClientHello 时，存在一个 NULL 指针取消引用缺陷。这使得远程攻击者可以使用意外的握手来崩溃守护进程，从而导致分布式拒绝服务攻击攻击。(CVE-2014-3569)-BIGNUM 平方(BN \_ sqr)实现没有正确计算 BIGNUM 值的平方。这使得远程攻击者可以击败加密保护机制。(CVE-2014-3570)-当处理 dtls1 \_ get \_ record ()消息时，存在一个 NULL 指针解引用缺陷。一个远程攻击者，使用一个特制的 DTLS 消息，可以导致一个分布式拒绝服务攻击。(CVE-2014-3571)-当使用没有 ServerKeyExchange 消息的 ECDSA 证书时，ECDH 握手存在缺陷。这允许远程攻击者触发来自密码套件的前向保密丢失。(CVE-2014-3572)-在接受证书签名算法和签名编码的非 der 变体时存在缺陷，原因是没有强制执行已签名和未签名部分之间的匹配。远程攻击者通过在证书的未签名部分包含精心制作的数据，可以绕过基于指纹的证书黑名单保护机制。(CVE-2014-8275)-一种安全特性绕过漏洞，称为 FREAK (对 RSA-EXPORT 密钥的因式分解攻击) ，由于支持密钥小于或等于512位的弱 EXPORT \_ rsa 密码套件而存在。中间人攻击者可以降低 SSL/TLS 连接的等级，使用 EXPORT \_ rsa 密码组合，该组合可以在短时间内分解，允许攻击者拦截和解密流量。(CVE-2015-0204)-在没有认证验证消息的情况下接受用于客户端身份验证的 DH 证书存在缺陷。这允许远程攻击者在没有私钥的情况下对服务进行身份验证。(CVE-2015-0205)-当处理包含相同数字序列但下一个历元的 DTLS 记录的饱和时，dtls1\_buffer \_ record ()发生内存泄漏。这使得远程攻击者可以引发分布式拒绝服务攻击攻击。(CVE-2015-0206)-由于在导入过程中对格式错误的 EC 私钥文件处理不当，d2i \_ ecprivatedkey ()函数中存在一个 use-after-free 条件。远程攻击者可以利用这一点取消引用或释放已释放的内存，从而导致分布式拒绝服务攻击或其他未指定的影响。(CVE-2015-0209)-ASN1 \_ type \_ cmp ()函数中存在无效的读缺陷，原因是布尔类型比较执行不当。远程攻击者可以利用这一点，通过一个精心设计的 x. 509证书到一个使用证书验证特性的端点，导致一个无效的读操作，造成一个分布式拒绝服务攻击。(CVE-2015-0286)-ASN1 \_ item \_ ex \_ d2i ()函数中存在一个缺陷，原因是在 ASN. 1解析中重用结构时未能重新初始化“ CHOICE”和“ ADB”数据结构。这允许远程攻击者造成无效的写操作和内存损坏，从而导致分布式拒绝服务攻击攻击。(CVE-2015-0287)-由于证书密钥处理不当，X509 \_ to \_ X509 \_ req ()函数中存在空指针解引用缺陷。这允许远程攻击者通过一个精心设计的 x. 509证书，引发一个分布式拒绝服务攻击攻击。(CVE-2015-0288)-由于错误处理丢失的外部 ContentInfo，PKCS # 7解析代码中存在 NULL 指针解引用缺陷。这允许远程攻击者使用处理任意 PKCS # 7数据的应用程序，并使用 ASN. 1编码提供格式不正确的数据，从而导致分布式拒绝服务攻击攻击。(CVE-2015-0289)-由于 SSLv2的实现不当，同时支持 SSLv2和启用导出密码套件的服务器中存在一个缺陷。远程攻击者可以利用这一点，通过一个精心设计的 CLIENT-MASTER-KEY 消息，引发分布式拒绝服务攻击攻击。(CVE-2015-0293)注意，Nessus 并没有尝试利用这些问题，而是仅仅依赖于应用程序的自我报告版本号。 | | | | | |
| **加固建议：**升级到 Apache Tomcat 7.0.60或更高版本。 | | | | | |
| Medium | Apache Tomcat 7.0. x < 7.0.60多个漏洞(FREAK) | CVE-2015-0286 | 6.8 | tcp | 8080 |
| **漏洞描述：**根据其自我报告的版本号，监听远程主机的 Apache Tomcat 服务在7.0.60之前是7.0.x。因此，它受到以下漏洞的影响:-当 SSLv3选项未启用且接收到 SSLv3 ClientHello 时，存在 NULL 指针解引用缺陷。这使得远程攻击者可以使用意外的握手来崩溃守护进程，从而导致分布式拒绝服务攻击攻击。(CVE-2014-3569)-BIGNUM 平方(BN \_ sqr)实现没有正确计算 BIGNUM 值的平方。这使得远程攻击者可以击败加密保护机制。(CVE-2014-3570)-在处理 DTLS 消息时，使用 dtls1 \_ get \_ record ()存在一个 NULL 指针解引用缺陷。一个远程攻击者，使用一个特制的 DTLS 消息，可以导致一个分布式拒绝服务攻击。(CVE-2014-3571)-当使用没有 ServerKeyExchange 消息的 ECDSA 证书时，ECDH 握手存在缺陷。这允许远程攻击者触发来自密码套件的前向保密丢失。(CVE-2014-3572)-在接受证书签名算法和签名编码的非 der 变体时存在缺陷，原因是没有强制执行已签名和未签名部分之间的匹配。远程攻击者通过在证书的未签名部分包含精心制作的数据，可以绕过基于指纹的证书黑名单保护机制。(CVE-2014-8275)-一个安全特性绕过漏洞，被称为 FREAK (对 RSA-EXPORT 密钥的因式分解攻击) ，由于支持密钥小于或等于512位的弱 EXPORT \_ rsa 密码套件而存在。中间人攻击者可以降低 SSL/TLS 连接的等级，使用 EXPORT \_ rsa 密码组合，该组合可以在短时间内分解，允许攻击者拦截和解密流量。(CVE-2015-0204)-在没有认证验证消息的情况下接受客户端身份验证的 DH 证书存在缺陷。这允许远程攻击者在没有私钥的情况下对服务进行身份验证。(CVE-2015-0205)-当处理包含相同数字序列但下一个历元的 DTLS 记录的饱和时，dtls1\_buffer \_ record ()发生内存泄漏。这使得远程攻击者可以引发分布式拒绝服务攻击攻击。(CVE-2015-0206)-由于在导入过程中对格式错误的 EC 私钥文件处理不当，d2i \_ ecprivatedkey ()函数中存在一个 use-after-free 条件。远程攻击者可以利用这一点取消引用或释放已释放的内存，从而导致分布式拒绝服务攻击或其他未指定的影响。(CVE-2015-0209)-ASN1 \_ type \_ cmp ()函数中存在无效的读缺陷，原因是布尔类型比较执行不当。远程攻击者可以利用这一点，通过一个精心设计的 x. 509证书到一个使用证书验证特性的端点，导致一个无效的读操作，造成一个分布式拒绝服务攻击。(CVE-2015-0286)-ASN1 \_ item \_ ex \_ d2i ()函数中存在一个缺陷，原因是在 ASN. 1解析中重用结构时未能重新初始化“ CHOICE”和“ ADB”数据结构。这允许远程攻击者造成无效的写操作和内存损坏，从而导致分布式拒绝服务攻击攻击。(CVE-2015-0287)-由于证书密钥处理不当，X509 \_ to \_ X509 \_ req ()函数中存在空指针解引用缺陷。这允许远程攻击者通过一个精心设计的 x. 509证书，引发一个分布式拒绝服务攻击攻击。(CVE-2015-0288)-由于错误处理丢失的外部 ContentInfo，PKCS # 7解析代码中存在 NULL 指针解引用缺陷。这允许远程攻击者使用处理任意 PKCS # 7数据的应用程序，并使用 ASN. 1编码提供格式不正确的数据，从而导致分布式拒绝服务攻击攻击。(CVE-2015-0289)-由于 SSLv2的实现不当，同时支持 SSLv2和启用导出密码套件的服务器中存在一个缺陷。远程攻击者可以利用这一点，通过一个精心设计的 CLIENT-MASTER-KEY 消息，引发分布式拒绝服务攻击攻击。(CVE-2015-0293)注意，Nessus 并没有尝试利用这些问题，而是仅仅依赖于应用程序的自我报告版本号。 | | | | | |
| **加固建议：**升级到 Apache Tomcat 7.0.60或更高版本。 | | | | | |
| Medium | Apache Tomcat 7.0. x < 7.0.60多个漏洞(FREAK) | CVE-2015-0287 | 6.8 | tcp | 8080 |
| **漏洞描述：**根据其自我报告的版本号，监听远程主机的 Apache Tomcat 服务在7.0.60之前是7.0.x。因此，它受到以下漏洞的影响:-当 SSLv3选项未启用且接收到 SSLv3 ClientHello 时，存在一个 NULL 指针取消引用缺陷。这使得远程攻击者可以使用意外的握手来崩溃守护进程，从而导致分布式拒绝服务攻击攻击。(CVE-2014-3569)-BIGNUM 平方(BN \_ sqr)实现没有正确计算 BIGNUM 值的平方。这使得远程攻击者可以击败加密保护机制。(CVE-2014-3570)-当处理 dtls1 \_ get \_ record ()消息时，存在一个 NULL 指针解引用缺陷。一个远程攻击者，使用一个特制的 DTLS 消息，可以导致一个分布式拒绝服务攻击。(CVE-2014-3571)-当使用没有 ServerKeyExchange 消息的 ECDSA 证书时，ECDH 握手存在缺陷。这允许远程攻击者触发来自密码套件的前向保密丢失。(CVE-2014-3572)-在接受证书签名算法和签名编码的非 der 变体时存在缺陷，原因是没有强制执行已签名和未签名部分之间的匹配。远程攻击者通过在证书的未签名部分包含精心制作的数据，可以绕过基于指纹的证书黑名单保护机制。(CVE-2014-8275)-一种安全特性绕过漏洞，称为 FREAK (对 RSA-EXPORT 密钥的因式分解攻击) ，由于支持密钥小于或等于512位的弱 EXPORT \_ rsa 密码套件而存在。中间人攻击者可以降低 SSL/TLS 连接的等级，使用 EXPORT \_ rsa 密码组合，该组合可以在短时间内分解，允许攻击者拦截和解密流量。(CVE-2015-0204)-在没有认证验证消息的情况下接受用于客户端身份验证的 DH 证书存在缺陷。这允许远程攻击者在没有私钥的情况下对服务进行身份验证。(CVE-2015-0205)-当处理包含相同数字序列但下一个历元的 DTLS 记录的饱和时，dtls1\_buffer \_ record ()发生内存泄漏。这使得远程攻击者可以引发分布式拒绝服务攻击攻击。(CVE-2015-0206)-由于在导入过程中对格式错误的 EC 私钥文件处理不当，d2i \_ ecprivatedkey ()函数中存在一个 use-after-free 条件。远程攻击者可以利用这一点取消引用或释放已释放的内存，从而导致分布式拒绝服务攻击或其他未指定的影响。(CVE-2015-0209)-ASN1 \_ type \_ cmp ()函数中存在无效的读缺陷，原因是布尔类型比较执行不当。远程攻击者可以利用这一点，通过一个精心设计的 x. 509证书到一个使用证书验证特性的端点，导致一个无效的读操作，造成一个分布式拒绝服务攻击。(CVE-2015-0286)-ASN1 \_ item \_ ex \_ d2i ()函数中存在一个缺陷，原因是在 ASN. 1解析中重用结构时未能重新初始化“ CHOICE”和“ ADB”数据结构。这允许远程攻击者造成无效的写操作和内存损坏，从而导致分布式拒绝服务攻击攻击。(CVE-2015-0287)-由于证书密钥处理不当，X509 \_ to \_ X509 \_ req ()函数中存在空指针解引用缺陷。这允许远程攻击者通过一个精心设计的 x. 509证书，引发一个分布式拒绝服务攻击攻击。(CVE-2015-0288)-由于错误处理丢失的外部 ContentInfo，PKCS # 7解析代码中存在 NULL 指针解引用缺陷。这允许远程攻击者使用处理任意 PKCS # 7数据的应用程序，并使用 ASN. 1编码提供格式不正确的数据，从而导致分布式拒绝服务攻击攻击。(CVE-2015-0289)-由于 SSLv2的实现不当，同时支持 SSLv2和启用导出密码套件的服务器中存在一个缺陷。远程攻击者可以利用这一点，通过一个精心设计的 CLIENT-MASTER-KEY 消息，引发分布式拒绝服务攻击攻击。(CVE-2015-0293)注意，Nessus 并没有尝试利用这些问题，而是仅仅依赖于应用程序的自我报告版本号。 | | | | | |
| **加固建议：**升级到 Apache Tomcat 7.0.60或更高版本。 | | | | | |
| Medium | Apache Tomcat 7.0. x < 7.0.60多个漏洞(FREAK) | CVE-2015-0288 | 6.8 | tcp | 8080 |
| **漏洞描述：**根据其自我报告的版本号，监听远程主机的 Apache Tomcat 服务在7.0.60之前是7.0.x。因此，它受到以下漏洞的影响:-当 SSLv3选项未启用且接收到 SSLv3 ClientHello 时，存在一个 NULL 指针取消引用缺陷。这使得远程攻击者可以使用意外的握手来崩溃守护进程，从而导致分布式拒绝服务攻击攻击。(CVE-2014-3569)-BIGNUM 平方(BN \_ sqr)实现没有正确计算 BIGNUM 值的平方。这使得远程攻击者可以击败加密保护机制。(CVE-2014-3570)-当处理 dtls1 \_ get \_ record ()消息时，存在一个 NULL 指针解引用缺陷。一个远程攻击者，使用一个特制的 DTLS 消息，可以导致一个分布式拒绝服务攻击。(CVE-2014-3571)-当使用没有 ServerKeyExchange 消息的 ECDSA 证书时，ECDH 握手存在缺陷。这允许远程攻击者触发来自密码套件的前向保密丢失。(CVE-2014-3572)-在接受证书签名算法和签名编码的非 der 变体时存在缺陷，原因是没有强制执行已签名和未签名部分之间的匹配。远程攻击者通过在证书的未签名部分包含精心制作的数据，可以绕过基于指纹的证书黑名单保护机制。(CVE-2014-8275)-一种安全特性绕过漏洞，称为 FREAK (对 RSA-EXPORT 密钥的因式分解攻击) ，由于支持密钥小于或等于512位的弱 EXPORT \_ rsa 密码套件而存在。中间人攻击者可以降低 SSL/TLS 连接的等级，使用 EXPORT \_ rsa 密码组合，该组合可以在短时间内分解，允许攻击者拦截和解密流量。(CVE-2015-0204)-在没有认证验证消息的情况下接受用于客户端身份验证的 DH 证书存在缺陷。这允许远程攻击者在没有私钥的情况下对服务进行身份验证。(CVE-2015-0205)-当处理包含相同数字序列但下一个历元的 DTLS 记录的饱和时，dtls1\_buffer \_ record ()发生内存泄漏。这使得远程攻击者可以引发分布式拒绝服务攻击攻击。(CVE-2015-0206)-由于在导入过程中对格式错误的 EC 私钥文件处理不当，d2i \_ ecprivatedkey ()函数中存在一个 use-after-free 条件。远程攻击者可以利用这一点取消引用或释放已释放的内存，从而导致分布式拒绝服务攻击或其他未指定的影响。(CVE-2015-0209)-ASN1 \_ type \_ cmp ()函数中存在无效的读缺陷，原因是布尔类型比较执行不当。远程攻击者可以利用这一点，通过一个精心设计的 x. 509证书到一个使用证书验证特性的端点，导致一个无效的读操作，造成一个分布式拒绝服务攻击。(CVE-2015-0286)-ASN1 \_ item \_ ex \_ d2i ()函数中存在一个缺陷，原因是在 ASN. 1解析中重用结构时未能重新初始化“ CHOICE”和“ ADB”数据结构。这允许远程攻击者造成无效的写操作和内存损坏，从而导致分布式拒绝服务攻击攻击。(CVE-2015-0287)-由于证书密钥处理不当，X509 \_ to \_ X509 \_ req ()函数中存在空指针解引用缺陷。这允许远程攻击者通过一个精心设计的 x. 509证书，引发一个分布式拒绝服务攻击攻击。(CVE-2015-0288)-由于错误处理丢失的外部 ContentInfo，PKCS # 7解析代码中存在 NULL 指针解引用缺陷。这允许远程攻击者使用处理任意 PKCS # 7数据的应用程序，并使用 ASN. 1编码提供格式不正确的数据，从而导致分布式拒绝服务攻击攻击。(CVE-2015-0289)-由于 SSLv2的实现不当，同时支持 SSLv2和启用导出密码套件的服务器中存在一个缺陷。远程攻击者可以利用这一点，通过一个精心设计的 CLIENT-MASTER-KEY 消息，引发分布式拒绝服务攻击攻击。(CVE-2015-0293)注意，Nessus 并没有尝试利用这些问题，而是仅仅依赖于应用程序的自我报告版本号。 | | | | | |
| **加固建议：**升级到 Apache Tomcat 7.0.60或更高版本。 | | | | | |
| Medium | Apache Tomcat 7.0. x < 7.0.60多个漏洞(FREAK) | CVE-2015-0289 | 6.8 | tcp | 8080 |
| **漏洞描述：**根据其自我报告的版本号，监听远程主机的 Apache Tomcat 服务在7.0.60之前是7.0.x。因此，它受到以下漏洞的影响:-当 SSLv3选项未启用且接收到 SSLv3 ClientHello 时，存在一个 NULL 指针取消引用缺陷。这使得远程攻击者可以使用意外的握手来崩溃守护进程，从而导致分布式拒绝服务攻击攻击。(CVE-2014-3569)-BIGNUM 平方(BN \_ sqr)实现没有正确计算 BIGNUM 值的平方。这使得远程攻击者可以击败加密保护机制。(CVE-2014-3570)-当处理 dtls1 \_ get \_ record ()消息时，存在一个 NULL 指针解引用缺陷。一个远程攻击者，使用一个特制的 DTLS 消息，可以导致一个分布式拒绝服务攻击。(CVE-2014-3571)-当使用没有 ServerKeyExchange 消息的 ECDSA 证书时，ECDH 握手存在缺陷。这允许远程攻击者触发来自密码套件的前向保密丢失。(CVE-2014-3572)-在接受证书签名算法和签名编码的非 der 变体时存在缺陷，原因是没有强制执行已签名和未签名部分之间的匹配。远程攻击者通过在证书的未签名部分包含精心制作的数据，可以绕过基于指纹的证书黑名单保护机制。(CVE-2014-8275)-一种安全特性绕过漏洞，称为 FREAK (对 RSA-EXPORT 密钥的因式分解攻击) ，由于支持密钥小于或等于512位的弱 EXPORT \_ rsa 密码套件而存在。中间人攻击者可以降低 SSL/TLS 连接的等级，使用 EXPORT \_ rsa 密码组合，该组合可以在短时间内分解，允许攻击者拦截和解密流量。(CVE-2015-0204)-在没有认证验证消息的情况下接受用于客户端身份验证的 DH 证书存在缺陷。这允许远程攻击者在没有私钥的情况下对服务进行身份验证。(CVE-2015-0205)-当处理包含相同数字序列但下一个历元的 DTLS 记录的饱和时，dtls1\_buffer \_ record ()发生内存泄漏。这使得远程攻击者可以引发分布式拒绝服务攻击攻击。(CVE-2015-0206)-由于在导入过程中对格式错误的 EC 私钥文件处理不当，d2i \_ ecprivatedkey ()函数中存在一个 use-after-free 条件。远程攻击者可以利用这一点取消引用或释放已释放的内存，从而导致分布式拒绝服务攻击或其他未指定的影响。(CVE-2015-0209)-ASN1 \_ type \_ cmp ()函数中存在无效的读缺陷，原因是布尔类型比较执行不当。远程攻击者可以利用这一点，通过一个精心设计的 x. 509证书到一个使用证书验证特性的端点，导致一个无效的读操作，造成一个分布式拒绝服务攻击。(CVE-2015-0286)-ASN1 \_ item \_ ex \_ d2i ()函数中存在一个缺陷，原因是在 ASN. 1解析中重用结构时未能重新初始化“ CHOICE”和“ ADB”数据结构。这允许远程攻击者造成无效的写操作和内存损坏，从而导致分布式拒绝服务攻击攻击。(CVE-2015-0287)-由于证书密钥处理不当，X509 \_ to \_ X509 \_ req ()函数中存在空指针解引用缺陷。这允许远程攻击者通过一个精心设计的 x. 509证书，引发一个分布式拒绝服务攻击攻击。(CVE-2015-0288)-由于错误处理丢失的外部 ContentInfo，PKCS # 7解析代码中存在 NULL 指针解引用缺陷。这允许远程攻击者使用处理任意 PKCS # 7数据的应用程序，并使用 ASN. 1编码提供格式不正确的数据，从而导致分布式拒绝服务攻击攻击。(CVE-2015-0289)-由于 SSLv2的实现不当，同时支持 SSLv2和启用导出密码套件的服务器中存在一个缺陷。远程攻击者可以利用这一点，通过一个精心设计的 CLIENT-MASTER-KEY 消息，引发分布式拒绝服务攻击攻击。(CVE-2015-0293)注意，Nessus 并没有尝试利用这些问题，而是仅仅依赖于应用程序的自我报告版本号。 | | | | | |
| **加固建议：**升级到 Apache Tomcat 7.0.60或更高版本。 | | | | | |
| Medium | Apache Tomcat 7.0. x < 7.0.60多个漏洞(FREAK) | CVE-2015-0293 | 6.8 | tcp | 8080 |
| **漏洞描述：**根据其自我报告的版本号，监听远程主机的 Apache Tomcat 服务在7.0.60之前是7.0.x。因此，它受到以下漏洞的影响:-当 SSLv3选项未启用且接收到 SSLv3 ClientHello 时，存在一个 NULL 指针取消引用缺陷。这使得远程攻击者可以使用意外的握手来崩溃守护进程，从而导致分布式拒绝服务攻击攻击。(CVE-2014-3569)-BIGNUM 平方(BN \_ sqr)实现没有正确计算 BIGNUM 值的平方。这使得远程攻击者可以击败加密保护机制。(CVE-2014-3570)-当处理 dtls1 \_ get \_ record ()消息时，存在一个 NULL 指针解引用缺陷。一个远程攻击者，使用一个特制的 DTLS 消息，可以导致一个分布式拒绝服务攻击。(CVE-2014-3571)-当使用没有 ServerKeyExchange 消息的 ECDSA 证书时，ECDH 握手存在缺陷。这允许远程攻击者触发来自密码套件的前向保密丢失。(CVE-2014-3572)-在接受证书签名算法和签名编码的非 der 变体时存在缺陷，原因是没有强制执行已签名和未签名部分之间的匹配。远程攻击者通过在证书的未签名部分包含精心制作的数据，可以绕过基于指纹的证书黑名单保护机制。(CVE-2014-8275)-一种安全特性绕过漏洞，称为 FREAK (对 RSA-EXPORT 密钥的因式分解攻击) ，由于支持密钥小于或等于512位的弱 EXPORT \_ rsa 密码套件而存在。中间人攻击者可以降低 SSL/TLS 连接的等级，使用 EXPORT \_ rsa 密码组合，该组合可以在短时间内分解，允许攻击者拦截和解密流量。(CVE-2015-0204)-在没有认证验证消息的情况下接受用于客户端身份验证的 DH 证书存在缺陷。这允许远程攻击者在没有私钥的情况下对服务进行身份验证。(CVE-2015-0205)-当处理包含相同数字序列但下一个历元的 DTLS 记录的饱和时，dtls1\_buffer \_ record ()发生内存泄漏。这使得远程攻击者可以引发分布式拒绝服务攻击攻击。(CVE-2015-0206)-由于在导入过程中对格式错误的 EC 私钥文件处理不当，d2i \_ ecprivatedkey ()函数中存在一个 use-after-free 条件。远程攻击者可以利用这一点取消引用或释放已释放的内存，从而导致分布式拒绝服务攻击或其他未指定的影响。(CVE-2015-0209)-ASN1 \_ type \_ cmp ()函数中存在无效的读缺陷，原因是布尔类型比较执行不当。远程攻击者可以利用这一点，通过一个精心设计的 x. 509证书到一个使用证书验证特性的端点，导致一个无效的读操作，造成一个分布式拒绝服务攻击。(CVE-2015-0286)-ASN1 \_ item \_ ex \_ d2i ()函数中存在一个缺陷，原因是在 ASN. 1解析中重用结构时未能重新初始化“ CHOICE”和“ ADB”数据结构。这允许远程攻击者造成无效的写操作和内存损坏，从而导致分布式拒绝服务攻击攻击。(CVE-2015-0287)-由于证书密钥处理不当，X509 \_ to \_ X509 \_ req ()函数中存在空指针解引用缺陷。这允许远程攻击者通过一个精心设计的 x. 509证书，引发一个分布式拒绝服务攻击攻击。(CVE-2015-0288)-由于错误处理丢失的外部 ContentInfo，PKCS # 7解析代码中存在 NULL 指针解引用缺陷。这允许远程攻击者使用处理任意 PKCS # 7数据的应用程序，并使用 ASN. 1编码提供格式不正确的数据，从而导致分布式拒绝服务攻击攻击。(CVE-2015-0289)-由于 SSLv2的实现不当，同时支持 SSLv2和启用导出密码套件的服务器中存在一个缺陷。远程攻击者可以利用这一点，通过一个精心设计的 CLIENT-MASTER-KEY 消息，引发分布式拒绝服务攻击攻击。(CVE-2015-0293)注意，Nessus 并没有尝试利用这些问题，而是仅仅依赖于应用程序的自我报告版本号。 | | | | | |
| **加固建议：**升级到 Apache Tomcat 7.0.60或更高版本。 | | | | | |
| Medium | MS16-047: SAM 和 LSAD 远程协议的安全更新(3148527)(Badlock)(未授权检查) | CVE-2016-0128 | 5.8 | tcp | 49157 |
| **漏洞描述：**由于远程过程调用(RPC)信道上的身份验证级别协商不当，安全帐户管理器(SAM)和本地安全权限(域策略)协议中的特权漏洞会增加，从而影响远程 Windows 主机。一个中间人攻击者能够拦截客户端和托管 SAM 数据库的服务器之间的通信，他可以利用这一点迫使认证级别降低，从而允许攻击者冒充一个经过认证的用户并访问 SAM 数据库。 | | | | | |
| **加固建议：**微软已经为 Windows Vista，2008,7,2008 r 2,2012,8.1，RT 8.1,2012 r 2和10发布了一系列补丁。 | | | | | |
| Medium | 1.0协议检测 |  | 6.1 | tcp | 3389 |
| **漏洞描述：**远程服务接受使用 TLS 1.0加密的连接。TLS 1.0有许多密码设计缺陷。TLS 1.0的现代实现缓解了这些问题，但是像1.2和1.3这样的 TLS 的新版本是针对这些缺陷设计的，应该尽可能地使用。截至2020年3月31日，不支持 TLS 1.2及以上版本的 Endpoints 在主流浏览器和主流厂商中将无法正常运行。PCI DSS v3.2要求在2018年6月30日之前完全禁用 TLS 1.0，但 POS POI 终端(以及它们连接的 SSL/TLS 终端点)可以被验证为不受任何已知漏洞的影响。 | | | | | |
| **加固建议：**启用对 TLS 1.2和1.3的支持，禁用对 TLS 1.0的支持。 | | | | | |
| Medium | 1.1协议检测 |  | 6.1 | tcp | 3389 |
| **漏洞描述：**远程服务接受使用 TLS 1.1加密的连接。TLS 1.1缺乏对当前和推荐的密码套件的支持。在 MAC 计算之前支持加密的加密器，以及认证加密模式，如 GCM 不能与 TLS 1.1一起使用。到2018年6月30日，PCI DSS v3.2仍然允许使用 TLS 1.1，但强烈建议使用 TLS 1.2。IETF 目前正在讨论一个完全不推荐 TLS 1.1的提议，许多供应商已经积极主动地这样做了。 | | | | | |
| **加固建议：**启用对 TLS 1.2和/或1.3的支持，并禁用 TLS 1.1的支持。 | | | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 低危 | 名称 | CVE | CVSS | protocol | port |
| Low | 终端服务加密级别与 FIPS-140不兼容 |  | 2.6 | tcp | 3389 |
| **漏洞描述：**远程终端服务使用的加密设置与 FIPS-140不兼容。 | | | | | |
| **加固建议：**将 RDP 加密级别更改为: 4. FIPS 兼容 | | | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 信息 | 名称 | CVE | CVSS | protocol | port |
| Info | 服务器类型和版本 |  |  | tcp | 80 |
| **漏洞描述：**这个插件试图确定远程网络服务器的类型和版本。 | | | | | |
| Info | 服务器类型和版本 |  |  | tcp | 81 |
| **漏洞描述：**这个插件试图确定远程网络服务器的类型和版本。 | | | | | |
| Info | 服务器类型和版本 |  |  | tcp | 82 |
| **漏洞描述：**这个插件试图确定远程网络服务器的类型和版本。 | | | | | |
| Info | 服务器类型和版本 |  |  | tcp | 83 |
| **漏洞描述：**这个插件试图确定远程网络服务器的类型和版本。 | | | | | |
| Info | 服务器类型和版本 |  |  | tcp | 8080 |
| **漏洞描述：**这个插件试图确定远程网络服务器的类型和版本。 | | | | | |
| Info | 请求远程日期披露 | CVE-1999-0524 | 0.0 | icmp | 0 |
| **漏洞描述：**远程主机应答 ICMP 时间戳请求。这允许攻击者知道目标计算机上设置的日期，这可能有助于未经身份验证的远程攻击者击败基于时间的身份验证协议。从运行 Windows Vista/7/2008/2008 R2的计算机返回的时间戳故意不正确，但通常在实际系统时间的1000秒内。 | | | | | |
| **加固建议：**筛选出 ICMP 时间戳请求(13)和传出 ICMP 时间戳答复(14)。 | | | | | |
| Info | Windows NetBIOS/SMB 远程主机信息披露 |  |  | udp | 137 |
| **漏洞描述：**远程主机正在侦听 UDP 端口137或 TCP 端口445，并响应 NetBIOS nbtscan 或 SMB 请求。请注意，这个插件收集的信息将用于其他插件，但本身不生成报告。 | | | | | |
| Info | Traceroute Information |  |  | udp | 0 |
| **漏洞描述：**向远程主机生成一个 traceroute。 | | | | | |
| Info | DCE 服务枚举 |  |  | tcp | 135 |
| **漏洞描述：**通过向端口映射器(TCP 135或 epmapper PIPE)发送查找请求，可以枚举在远程端口上运行的分散式运算环境服务(DCE)。通过使用此信息，可以通过向远程端口/管道发送 RPC 请求来连接和绑定到每个服务。 | | | | | |
| Info | DCE 服务枚举 |  |  | tcp | 445 |
| **漏洞描述：**通过向端口映射器(TCP 135或 epmapper PIPE)发送查找请求，可以枚举在远程端口上运行的分散式运算环境服务(DCE)。通过使用此信息，可以通过向远程端口/管道发送 RPC 请求来连接和绑定到每个服务。 | | | | | |
| Info | DCE 服务枚举 |  |  | tcp | 2103 |
| **漏洞描述：**通过向端口映射器(TCP 135或 epmapper PIPE)发送查找请求，可以枚举在远程端口上运行的分散式运算环境服务(DCE)。通过使用此信息，可以通过向远程端口/管道发送 RPC 请求来连接和绑定到每个服务。 | | | | | |
| Info | DCE 服务枚举 |  |  | tcp | 2105 |
| **漏洞描述：**通过向端口映射器(TCP 135或 epmapper PIPE)发送查找请求，可以枚举在远程端口上运行的分散式运算环境服务(DCE)。通过使用此信息，可以通过向远程端口/管道发送 RPC 请求来连接和绑定到每个服务。 | | | | | |
| Info | DCE 服务枚举 |  |  | tcp | 2107 |
| **漏洞描述：**通过向端口映射器(TCP 135或 epmapper PIPE)发送查找请求，可以枚举在远程端口上运行的分散式运算环境服务(DCE)。通过使用此信息，可以通过向远程端口/管道发送 RPC 请求来连接和绑定到每个服务。 | | | | | |
| Info | DCE 服务枚举 |  |  | tcp | 49152 |
| **漏洞描述：**通过向端口映射器(TCP 135或 epmapper PIPE)发送查找请求，可以枚举在远程端口上运行的分散式运算环境服务(DCE)。通过使用此信息，可以通过向远程端口/管道发送 RPC 请求来连接和绑定到每个服务。 | | | | | |
| Info | DCE 服务枚举 |  |  | tcp | 49153 |
| **漏洞描述：**通过向端口映射器(TCP 135或 epmapper PIPE)发送查找请求，可以枚举在远程端口上运行的分散式运算环境服务(DCE)。通过使用此信息，可以通过向远程端口/管道发送 RPC 请求来连接和绑定到每个服务。 | | | | | |
| Info | DCE 服务枚举 |  |  | tcp | 49154 |
| **漏洞描述：**通过向端口映射器(TCP 135或 epmapper PIPE)发送查找请求，可以枚举在远程端口上运行的分散式运算环境服务(DCE)。通过使用此信息，可以通过向远程端口/管道发送 RPC 请求来连接和绑定到每个服务。 | | | | | |
| Info | DCE 服务枚举 |  |  | tcp | 49155 |
| **漏洞描述：**通过向端口映射器(TCP 135或 epmapper PIPE)发送查找请求，可以枚举在远程端口上运行的分散式运算环境服务(DCE)。通过使用此信息，可以通过向远程端口/管道发送 RPC 请求来连接和绑定到每个服务。 | | | | | |
| Info | DCE 服务枚举 |  |  | tcp | 49157 |
| **漏洞描述：**通过向端口映射器(TCP 135或 epmapper PIPE)发送查找请求，可以枚举在远程端口上运行的分散式运算环境服务(DCE)。通过使用此信息，可以通过向远程端口/管道发送 RPC 请求来连接和绑定到每个服务。 | | | | | |
| Info | DCE 服务枚举 |  |  | tcp | 49166 |
| **漏洞描述：**通过向端口映射器(TCP 135或 epmapper PIPE)发送查找请求，可以枚举在远程端口上运行的分散式运算环境服务(DCE)。通过使用此信息，可以通过向远程端口/管道发送 RPC 请求来连接和绑定到每个服务。 | | | | | |
| Info | DCE 服务枚举 |  |  | tcp | 49167 |
| **漏洞描述：**通过向端口映射器(TCP 135或 epmapper PIPE)发送查找请求，可以枚举在远程端口上运行的分散式运算环境服务(DCE)。通过使用此信息，可以通过向远程端口/管道发送 RPC 请求来连接和绑定到每个服务。 | | | | | |
| Info | 远程系统信息披露 |  |  | tcp | 445 |
| **漏洞描述：**Nessus 能够通过向端口139或445发送身份验证请求来获得远程操作系统名称和版本(Windows 和/或 Samba)。注意，这个插件要求在主机上启用 SMB1。 | | | | | |
| Info | SSL 证书信息 |  |  | tcp | 3389 |
| **漏洞描述：**这个插件连接到每个 ssl 相关的端口，并尝试提取和转储 x. 509证书。 | | | | | |
| Info | 启用 Windows 终端服务 |  |  | tcp | 3389 |
| **漏洞描述：**终端服务允许 Windows 用户远程获得图形登录(因此作为远程主机上的本地用户)。如果攻击者获得了有效的登录名和密码，则可以使用此服务进一步访问远程主机。攻击者也可以使用这个服务向远程主机挂载一个字典式攻击文件夹来尝试远程登录。注意，RDP (远程桌面协议)容易受到中间人攻击，这使得攻击者很容易通过模拟 Windows 服务器窃取合法用户的证书。 | | | | | |
| **加固建议：**如果您不使用终端服务，请禁用该服务，并且不允许该服务在 Internet 上运行。 | | | | | |
| Info | 微软 Windows SMB 服务检测 |  |  | tcp | 139 |
| **漏洞描述：**远程服务理解 CIFS (公共互联网文件系统)或服务器消息块(SMB)协议，用于在网络节点之间提供对文件、打印机等的共享访问。 | | | | | |
| Info | 微软 Windows SMB 服务检测 |  |  | tcp | 445 |
| **漏洞描述：**远程服务理解 CIFS (公共互联网文件系统)或服务器消息块(SMB)协议，用于在网络节点之间提供对文件、打印机等的共享访问。 | | | | | |
| Info | Nessus SYN 扫描器 |  |  | tcp | 80 |
| **漏洞描述：**这个插件是一个 SYN’半开’端口扫描器。即使对付一个有防火墙的目标，它也应该相当迅速。请注意，SYN 扫描比 TCP (完全连接)扫描破坏的服务的干扰性要小，但是如果网络已经加载，SYN 扫描可能会对不那么健壮的防火墙造成问题，并且在远程目标上留下未关闭的连接。 | | | | | |
| **加固建议：**用 IP 过滤器保护你的目标。 | | | | | |
| Info | Nessus SYN 扫描器 |  |  | tcp | 81 |
| **漏洞描述：**这个插件是一个 SYN’半开’端口扫描器。即使对付一个有防火墙的目标，它也应该相当迅速。请注意，SYN 扫描比 TCP (完全连接)扫描破坏的服务的干扰性要小，但是如果网络已经加载，SYN 扫描可能会对不那么健壮的防火墙造成问题，并且在远程目标上留下未关闭的连接。 | | | | | |
| **加固建议：**用 IP 过滤器保护你的目标。 | | | | | |
| Info | Nessus SYN 扫描器 |  |  | tcp | 82 |
| **漏洞描述：**这个插件是一个 SYN’半开’端口扫描器。即使对付一个有防火墙的目标，它也应该相当迅速。请注意，SYN 扫描比 TCP (完全连接)扫描破坏的服务的干扰性要小，但是如果网络已经加载，SYN 扫描可能会对不那么健壮的防火墙造成问题，并且在远程目标上留下未关闭的连接。 | | | | | |
| **加固建议：**用 IP 过滤器保护你的目标。 | | | | | |
| Info | Nessus SYN 扫描器 |  |  | tcp | 83 |
| **漏洞描述：**这个插件是一个 SYN’半开’端口扫描器。即使对付一个有防火墙的目标，它也应该相当迅速。请注意，SYN 扫描比 TCP (完全连接)扫描破坏的服务的干扰性要小，但是如果网络已经加载，SYN 扫描可能会对不那么健壮的防火墙造成问题，并且在远程目标上留下未关闭的连接。 | | | | | |
| **加固建议：**用 IP 过滤器保护你的目标。 | | | | | |
| Info | Nessus SYN 扫描器 |  |  | tcp | 135 |
| **漏洞描述：**这个插件是一个 SYN’半开’端口扫描器。即使对付一个有防火墙的目标，它也应该相当迅速。请注意，SYN 扫描比 TCP (完全连接)扫描破坏的服务的干扰性要小，但是如果网络已经加载，SYN 扫描可能会对不那么健壮的防火墙造成问题，并且在远程目标上留下未关闭的连接。 | | | | | |
| **加固建议：**用 IP 过滤器保护你的目标。 | | | | | |
| Info | Nessus SYN 扫描器 |  |  | tcp | 139 |
| **漏洞描述：**这个插件是一个 SYN’半开’端口扫描器。即使对付一个有防火墙的目标，它也应该相当迅速。请注意，SYN 扫描比 TCP (完全连接)扫描破坏的服务的干扰性要小，但是如果网络已经加载，SYN 扫描可能会对不那么健壮的防火墙造成问题，并且在远程目标上留下未关闭的连接。 | | | | | |
| **加固建议：**用 IP 过滤器保护你的目标。 | | | | | |
| Info | Nessus SYN 扫描器 |  |  | tcp | 445 |
| **漏洞描述：**这个插件是一个 SYN’半开’端口扫描器。即使对付一个有防火墙的目标，它也应该相当迅速。请注意，SYN 扫描比 TCP (完全连接)扫描破坏的服务的干扰性要小，但是如果网络已经加载，SYN 扫描可能会对不那么健壮的防火墙造成问题，并且在远程目标上留下未关闭的连接。 | | | | | |
| **加固建议：**用 IP 过滤器保护你的目标。 | | | | | |
| Info | Nessus SYN 扫描器 |  |  | tcp | 1801 |
| **漏洞描述：**这个插件是一个 SYN’半开’端口扫描器。即使对付一个有防火墙的目标，它也应该相当迅速。请注意，SYN 扫描比 TCP (完全连接)扫描破坏的服务的干扰性要小，但是如果网络已经加载，SYN 扫描可能会对不那么健壮的防火墙造成问题，并且在远程目标上留下未关闭的连接。 | | | | | |
| **加固建议：**用 IP 过滤器保护你的目标。 | | | | | |
| Info | Nessus SYN 扫描器 |  |  | tcp | 2103 |
| **漏洞描述：**这个插件是一个 SYN’半开’端口扫描器。即使对付一个有防火墙的目标，它也应该相当迅速。请注意，SYN 扫描比 TCP (完全连接)扫描破坏的服务的干扰性要小，但是如果网络已经加载，SYN 扫描可能会对不那么健壮的防火墙造成问题，并且在远程目标上留下未关闭的连接。 | | | | | |
| **加固建议：**用 IP 过滤器保护你的目标。 | | | | | |
| Info | Nessus SYN 扫描器 |  |  | tcp | 2105 |
| **漏洞描述：**这个插件是一个 SYN’半开’端口扫描器。即使对付一个有防火墙的目标，它也应该相当迅速。请注意，SYN 扫描比 TCP (完全连接)扫描破坏的服务的干扰性要小，但是如果网络已经加载，SYN 扫描可能会对不那么健壮的防火墙造成问题，并且在远程目标上留下未关闭的连接。 | | | | | |
| **加固建议：**用 IP 过滤器保护你的目标。 | | | | | |
| Info | Nessus SYN 扫描器 |  |  | tcp | 2107 |
| **漏洞描述：**这个插件是一个 SYN’半开’端口扫描器。即使对付一个有防火墙的目标，它也应该相当迅速。请注意，SYN 扫描比 TCP (完全连接)扫描破坏的服务的干扰性要小，但是如果网络已经加载，SYN 扫描可能会对不那么健壮的防火墙造成问题，并且在远程目标上留下未关闭的连接。 | | | | | |
| **加固建议：**用 IP 过滤器保护你的目标。 | | | | | |
| Info | Nessus SYN 扫描器 |  |  | tcp | 3389 |
| **漏洞描述：**这个插件是一个 SYN’半开’端口扫描器。即使对付一个有防火墙的目标，它也应该相当迅速。请注意，SYN 扫描比 TCP (完全连接)扫描破坏的服务的干扰性要小，但是如果网络已经加载，SYN 扫描可能会对不那么健壮的防火墙造成问题，并且在远程目标上留下未关闭的连接。 | | | | | |
| **加固建议：**用 IP 过滤器保护你的目标。 | | | | | |
| Info | Nessus SYN 扫描器 |  |  | tcp | 8080 |
| **漏洞描述：**这个插件是一个 SYN’半开’端口扫描器。即使对付一个有防火墙的目标，它也应该相当迅速。请注意，SYN 扫描比 TCP (完全连接)扫描破坏的服务的干扰性要小，但是如果网络已经加载，SYN 扫描可能会对不那么健壮的防火墙造成问题，并且在远程目标上留下未关闭的连接。 | | | | | |
| **加固建议：**用 IP 过滤器保护你的目标。 | | | | | |
| Info | Web 服务器未配置-默认安装页面出现 |  |  | tcp | 80 |
| **漏洞描述：**远程 web 服务器使用其默认的欢迎页面。因此，这个服务器很可能根本没有被使用，或者正在提供本应被隐藏的内容。 | | | | | |
| **加固建议：**如果您不使用此服务，请关闭此服务。 | | | | | |
| Info | Web 服务器未配置-默认安装页面出现 |  |  | tcp | 8080 |
| **漏洞描述：**远程 web 服务器使用其默认的欢迎页面。因此，这个服务器很可能根本没有被使用，或者正在提供本应被隐藏的内容。 | | | | | |
| **加固建议：**如果您不使用此服务，请关闭此服务。 | | | | | |
| Info | 操作系统识别 |  |  | tcp | 0 |
| **漏洞描述：**使用远程探测的组合(例如，TCP/IP、 SMB、 HTTP、 NTP、 SNMP 等) ，可以猜测正在使用的远程操作系统的名称。有时也可以猜测操作系统的版本。 | | | | | |
| Info | Nessus 扫描信息 |  |  | tcp | 0 |
| **漏洞描述：**这个插件显示，对于每个被测试的主机，扫描本身的信息:-插件集的版本。- 扫描器的类型(Nessus 或 Nessus Home)。Nessus 引擎的版本。- 使用的端口扫描器。- 扫描的端口范围。- 是否可以进行授权或第三方补丁管理检查。- 扫描日期。- 扫描时间。- 同时扫描的主机数目。- 同时进行的检查次数。 | | | | | |
| Info | 虚拟机检测 |  |  | tcp | 0 |
| **漏洞描述：**根据其网络适配器的 MAC 地址，远程主机是一个 VMware 虚拟机。 | | | | | |
| **加固建议：**由于可以通过网络在物理上访问它，因此要确保其配置与组织的安全策略相匹配。 | | | | | |
| Info | Web 服务器/应用程序图标. ico 供应商指纹 |  |  | tcp | 8080 |
| **漏洞描述：**在远程 web 服务器上找到的 favicon.ico 文件属于一个流行的 web 服务器。这可能被用来指纹网络服务器。 | | | | | |
| **加固建议：**移除 favicon.ico 文件或为你的网站创建一个自定义文件。 | | | | | |
| Info | 支持 SSL 密码组合 |  |  | tcp | 3389 |
| **漏洞描述：**此插件检测远程服务支持哪些 SSL 加密器来加密通信。 | | | | | |
| Info | 服务侦测 |  |  | tcp | 80 |
| **漏洞描述：**Nessus 能够通过其旗帜或者在接收到 HTTP 请求时查看其发送的错误消息来识别远程服务。 | | | | | |
| Info | 服务侦测 |  |  | tcp | 81 |
| **漏洞描述：**Nessus 能够通过其旗帜或者在接收到 HTTP 请求时查看其发送的错误消息来识别远程服务。 | | | | | |
| Info | 服务侦测 |  |  | tcp | 82 |
| **漏洞描述：**Nessus 能够通过其旗帜或者在接收到 HTTP 请求时查看其发送的错误消息来识别远程服务。 | | | | | |
| Info | 服务侦测 |  |  | tcp | 83 |
| **漏洞描述：**Nessus 能够通过其旗帜或者在接收到 HTTP 请求时查看其发送的错误消息来识别远程服务。 | | | | | |
| Info | 服务侦测 |  |  | tcp | 8080 |
| **漏洞描述：**Nessus 能够通过其旗帜或者在接收到 HTTP 请求时查看其发送的错误消息来识别远程服务。 | | | | | |
| Info | 超文本传输协议信息 |  |  | tcp | 80 |
| **漏洞描述：**这个测试提供了一些关于远程 HTTP 协议的信息——使用的版本，是否启用了 HTTP Keep-Alive 和 HTTP 管道等等。.这个测试只是信息性的，并不表示任何安全问题。 | | | | | |
| Info | 超文本传输协议信息 |  |  | tcp | 81 |
| **漏洞描述：**这个测试提供了一些关于远程 HTTP 协议的信息——使用的版本，是否启用了 HTTP Keep-Alive 和 HTTP 管道等等。.这个测试只是信息性的，并不表示任何安全问题。 | | | | | |
| Info | 超文本传输协议信息 |  |  | tcp | 82 |
| **漏洞描述：**这个测试提供了一些关于远程 HTTP 协议的信息——使用的版本，是否启用了 HTTP Keep-Alive 和 HTTP 管道等等。.这个测试只是信息性的，并不表示任何安全问题。 | | | | | |
| Info | 超文本传输协议信息 |  |  | tcp | 83 |
| **漏洞描述：**这个测试提供了一些关于远程 HTTP 协议的信息——使用的版本，是否启用了 HTTP Keep-Alive 和 HTTP 管道等等。.这个测试只是信息性的，并不表示任何安全问题。 | | | | | |
| Info | 超文本传输协议信息 |  |  | tcp | 8080 |
| **漏洞描述：**这个测试提供了一些关于远程 HTTP 协议的信息——使用的版本，是否启用了 HTTP Keep-Alive 和 HTTP 管道等等。.这个测试只是信息性的，并不表示任何安全问题。 | | | | | |
| Info | 支持 TCP/IP 时间戳 |  |  | tcp | 0 |
| **漏洞描述：**远程主机实现 TCP 时间戳，如 RFC1323所定义的。这个特性的一个副作用是，有时可以计算远程主机的正常运行时间。 | | | | | |
| Info | 以太网卡制造商检测 |  |  | tcp | 0 |
| **漏洞描述：**每个以太网 MAC 地址都以一个24位组织唯一标识符开头。 | | | | | |
| Info | Apache Tomcat 检测 |  |  | tcp | 8080 |
| **漏洞描述：**Nessus 能够检测到远程 Apache Tomcat web 服务器。 | | | | | |
| Info | HTTP 方法允许(每个目录) |  |  | tcp | 80 |
| **漏洞描述：**通过调用 OPTIONS 方法，可以确定每个目录上允许使用哪些 HTTP 方法。下面的 HTTP 方法被认为是不安全的: PUT、 DELETE、 CONNECT、 TRACE、 HEAD 许多框架和语言将‘ HEAD’视为‘ GET’请求，尽管响应中没有任何主体。如果在“ GET”请求上设置了安全约束，只有“ authenticatedUsers”可以访问特定 servlet 或资源的 GET 请求，那么“ HEAD”版本将绕过该约束。这允许未经授权的盲目提交任何特权 GET 请求。由于这个列表可能不完整，插件还会测试每个目录上的各种已知 HTTP 方法，如果接收到的响应代码为400、403、405或501，插件还会测试是否启用了“彻底测试”或“启用 web 应用程序测试”在扫描策略中设置为“是”，并认为这些方法不受支持。注意，插件的输出只是信息性的，并不一定表明存在任何安全漏洞。 | | | | | |
| Info | HTTP 方法允许(每个目录) |  |  | tcp | 81 |
| **漏洞描述：**通过调用 OPTIONS 方法，可以确定每个目录上允许使用哪些 HTTP 方法。下面的 HTTP 方法被认为是不安全的: PUT、 DELETE、 CONNECT、 TRACE、 HEAD 许多框架和语言将‘ HEAD’视为‘ GET’请求，尽管响应中没有任何主体。如果在“ GET”请求上设置了安全约束，只有“ authenticatedUsers”可以访问特定 servlet 或资源的 GET 请求，那么“ HEAD”版本将绕过该约束。这允许未经授权的盲目提交任何特权 GET 请求。由于这个列表可能不完整，插件还会测试每个目录上的各种已知 HTTP 方法，如果接收到的响应代码为400、403、405或501，插件还会测试是否启用了“彻底测试”或“启用 web 应用程序测试”在扫描策略中设置为“是”，并认为这些方法不受支持。注意，插件的输出只是信息性的，并不一定表明存在任何安全漏洞。 | | | | | |
| Info | HTTP 方法允许(每个目录) |  |  | tcp | 82 |
| **漏洞描述：**通过调用 OPTIONS 方法，可以确定每个目录上允许使用哪些 HTTP 方法。下面的 HTTP 方法被认为是不安全的: PUT、 DELETE、 CONNECT、 TRACE、 HEAD 许多框架和语言将‘ HEAD’视为‘ GET’请求，尽管响应中没有任何主体。如果在“ GET”请求上设置了安全约束，只有“ authenticatedUsers”可以访问特定 servlet 或资源的 GET 请求，那么“ HEAD”版本将绕过该约束。这允许未经授权的盲目提交任何特权 GET 请求。由于这个列表可能不完整，插件还会测试每个目录上的各种已知 HTTP 方法，如果接收到的响应代码为400、403、405或501，插件还会测试是否启用了“彻底测试”或“启用 web 应用程序测试”在扫描策略中设置为“是”，并认为这些方法不受支持。注意，插件的输出只是信息性的，并不一定表明存在任何安全漏洞。 | | | | | |
| Info | HTTP 方法允许(每个目录) |  |  | tcp | 83 |
| **漏洞描述：**通过调用 OPTIONS 方法，可以确定每个目录上允许使用哪些 HTTP 方法。下面的 HTTP 方法被认为是不安全的: PUT、 DELETE、 CONNECT、 TRACE、 HEAD 许多框架和语言将‘ HEAD’视为‘ GET’请求，尽管响应中没有任何主体。如果在“ GET”请求上设置了安全约束，只有“ authenticatedUsers”可以访问特定 servlet 或资源的 GET 请求，那么“ HEAD”版本将绕过该约束。这允许未经授权的盲目提交任何特权 GET 请求。由于这个列表可能不完整，插件还会测试每个目录上的各种已知 HTTP 方法，如果接收到的响应代码为400、403、405或501，插件还会测试是否启用了“彻底测试”或“启用 web 应用程序测试”在扫描策略中设置为“是”，并认为这些方法不受支持。注意，插件的输出只是信息性的，并不一定表明存在任何安全漏洞。 | | | | | |
| Info | 公共平台枚举(CPE) |  |  | tcp | 0 |
| **漏洞描述：**通过使用从 Nessus 扫描获得的信息，这个插件报告 CPE (公共平台枚举)匹配主机上的各种硬件和软件产品。注意，如果产品没有官方的 CPE，这个插件会根据扫描得到的信息计算出最好的 CPE。 | | | | | |
| Info | 支持 SSL 会话恢复 |  |  | tcp | 3389 |
| **漏洞描述：**此脚本通过执行完整的 SSL 握手来检测主机是否允许恢复 SSL 会话，以接收会话 ID，然后重新连接到以前使用的会话 ID。如果服务器在第二个连接中接受会话 ID，则服务器维护一个会话缓存，可以继续进行。 | | | | | |
| Info | 设备类型 |  |  | tcp | 0 |
| **漏洞描述：**基于远程操作系统，可以确定远程系统类型(例如: 打印机、路由器、通用计算机等)。 | | | | | |
| Info | 支持 SSL/TLS 版本 |  |  | tcp | 3389 |
| **漏洞描述：**此插件检测哪些 SSL 和 TLS 版本支持远程服务，以便对通信进行加密。 | | | | | |
| Info | 支持 SSL/完备的前向安全性/密码套件 |  |  | tcp | 3389 |
| **漏洞描述：**远程主机支持使用 SSL 加密器，提供完备的前向安全性加密(PFS)。这些密码组合确保如果服务器的私钥受到破坏，那么在将来的某个日期，记录的 SSL 通信不会被破坏。 | | | | | |
| Info | 使用 SSL/TLS 的终端服务 |  |  | tcp | 3389 |
| **漏洞描述：**远程终端服务配置为使用 SSL/TLS。 | | | | | |
| Info | RDP 屏幕截图 |  |  | tcp | 3389 |
| **漏洞描述：**这个脚本试图通过 RDP (远程桌面协议)连接到远程主机，并试图截取登录屏幕的屏幕截图。虽然这本身并不是一个漏洞，但有些版本的 Windows 显示了可以连接的用户的姓名以及已经连接的用户的姓名。 | | | | | |
| Info | 补丁报告 |  |  | tcp | 0 |
| **漏洞描述：**远程主机缺少一个或多个安全补丁。这个插件列出了要安装的每个补丁的最新版本，以确保远程主机是最新的。 | | | | | |
| **加固建议：**安装下面列出的修补程序。 | | | | | |
| Info | 支持 SSL 密码块链接密码套件 |  |  | tcp | 3389 |
| **漏洞描述：**远程主机支持使用在 Cipher Block Chaining (CBC)模式下运行的 SSL 加密程序。这些密码套件比电子密码本(Electronic Codebook，ECB)模式提供了额外的安全性，但如果使用不当，则有可能泄露信息。 | | | | | |
| Info | 以太网 MAC 地址 |  |  | tcp | 0 |
| **漏洞描述：**这个插件收集从主机的远程探测(例如 SNMP 和 Netbios)和运行本地检查(例如 ifconfig)中发现的 MAC 地址。然后，它将 MAC 地址合并成一个单一的、唯一的和统一的列表。 | | | | | |
| Info | 服务器消息块(SMB)协议版本1已启用(未授权的检查) |  |  | tcp | 445 |
| **漏洞描述：**远程 Windows 主机支持服务器消息块协议版本1(SMBv1)。微软建议用户停止使用 SMBv1，因为后来的 SMB 版本中缺乏安全特性。此外，据报道影子经纪人组有一个漏洞会影响 SMB; 然而，这个漏洞是否会影响 SMBv1或其他版本尚不清楚。针对这个问题，US-CERT 建议用户禁用 SMBv1/SMB 最佳实践，以缓解这些潜在问题。 | | | | | |
| **加固建议：**根据 Microsoft KB2696547中的供应商指令禁用 SMBv1。此外，通过阻塞所有网络边界设备上的 TCP 端口445，直接阻塞 SMB。对于基于 NetBIOS API 的 SMB，在所有网络边界设备上阻止 TCP 端口137/139和 UDP 端口137/138。 | | | | | |
| Info | 支持 microsoftwindows SMB 版本(远程检查) |  |  | tcp | 445 |
| **漏洞描述：**Nessus 能够通过向端口139或445发送身份验证请求来获得在远程主机上运行的 SMB 版本。注意，这个插件是一个远程检查，不能在代理上工作。 | | | | | |
| Info | 支持 Microsoft Windows SMB2和 SMB3方言(远程检查) |  |  | tcp | 445 |
| **漏洞描述：**Nessus 可以通过向端口139或445发送一个身份验证请求来获得运行在远程主机上的 SMB2和 SMB3方言集。 | | | | | |
| Info | 没有提供证书 |  |  | tcp | 0 |
| **漏洞描述：**Nessus 无法执行凭证检查，因为没有提供凭证。 | | | | | |
| Info | 本地检查未启用(信息) |  |  | tcp | 0 |
| **漏洞描述：**Nessus 没有在远程主机上启用本地检查。这并不一定表明扫描有问题。可能没有提供凭证，可能无法为目标提供本地检查，可能没有识别目标，或者可能发生了另一个问题，阻止启用本地检查。详细信息请参阅插件输出。此插件报告与未启用本地检查有关的信息检查结果。有关失败信息，请参见插件21745: “身份验证失败-本地检查未运行”。 | | | | | |

## 192.168.59.10

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1 | 0 | 10 | 0 | 64 |
| **紧急** | **高危** | **中危** | **低危** | **信息** |

详细信息：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 紧急 | 名称 | CVE | CVSS | protocol | port |
| Critical | MS14-066: Schannel 中的漏洞可能允许远程代码执行(2992611)(未授权检查) | CVE-2014-6321 | 10.0 | tcp | 3389 |
| **漏洞描述：**由于安全通道(Schannel)安全包对数据包的处理不当，远程 Windows 主机受到远程代码执行漏洞的影响。攻击者可以通过向 Windows 服务器发送特制的包来利用这个问题。注意，这个插件发送一个客户端证书 TLS 握手消息，然后是 CertificateVerify 消息。一些 Windows 主机在接收到客户端证书时将关闭连接，而它并没有通过 CertificateRequest 消息请求客户端证书。在这种情况下，插件无法继续检测漏洞，因为 CertificateVerify 消息无法发送。 | | | | | |
| **加固建议：**微软已经为 Windows 2003，Vista，2008,7,2008 r 2,8,2012,8.1和2012 r 2发布了一系列补丁。 | | | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 中危 | 名称 | CVE | CVSS | protocol | port |
| Medium | 使用弱哈希算法签名的 SSL 证书 | CVE-2004-2761 | 5.0 | tcp | 3389 |
| **漏洞描述：**远程服务使用 SSL 证书链，该证书链使用加密弱散列算法(例如 MD2、 MD4、 MD5或 SHA1)进行签名。众所周知，这些签名算法容易受到碰撞攻击。攻击者可以利用这一点生成具有相同数字签名的另一个证书，从而允许攻击者伪装成受影响的服务。注意，这个插件报告所有用 SHA-1签署的 SSL 证书链在2017年1月1日之后过期是脆弱的。这是根据谷歌逐步取消 SHA-1加密散列算法。注意，证书链中包含在 Nessus CA 数据库(已知的 \_ CA)中。已经被忽视。 | | | | | |
| **加固建议：**联系证书颁发机构重新颁发证书。 | | | | | |
| Medium | 支持 SSL 中等强度密码组合(SWEET32) | CVE-2016-2183 | 5.0 | tcp | 3389 |
| **漏洞描述：**远程主机支持使用提供中等强度加密的 SSL 加密器。Nessus 认为中等强度的加密使用至少64位和小于112位的密钥长度，或者使用3DES 加密套件。请注意，如果攻击者位于同一物理网络上，那么绕过中等强度的加密要容易得多。 | | | | | |
| **加固建议：**重新配置受影响的应用程序，如果可能的话，避免使用中等强度的密码。 | | | | | |
| Medium | 不能信任 SSL 证书 |  | 6.4 | tcp | 3389 |
| **漏洞描述：**不能信任服务器的 x. 509证书。这种情况可能以三种不同的方式发生，其中可以破坏信任链，如下所述:-首先，服务器发送的证书链的顶端可能不是来自已知的公共证书颁发机构。这种情况可能发生在链的顶部是一个无法识别的自签名证书时，也可能发生在缺少将证书链的顶部连接到已知公共证书颁发机构的中间证书时。- 第二，证书链可能包含扫描时无效的证书。这可能发生在扫描发生在某个证书的“ notBefore”日期之前，或者发生在某个证书的“ notAfter”日期之后。- 第三，证书链可能包含与证书信息不匹配或无法验证的签名。错误签名可以通过获取带有错误签名的证书并由其签发者重新签名来修复。无法验证的签名是证书颁发者使用 Nessus 不支持或不认可的签名算法的结果。如果远程主机是生产环境中的公共主机，链路中的任何中断都会使用户更难以验证 web 服务器的真实性和身份。这使得对远程主机执行中间人攻击变得更加容易。 | | | | | |
| **加固建议：**为此服务购买或生成适当的证书。 | | | | | |
| Medium | 自签署证书 |  | 6.4 | tcp | 3389 |
| **漏洞描述：**此服务的 x. 509证书链不是由认可的证书颁发机构签名的。如果远程主机是生产环境中的公共主机，那么 SSL 的使用就无效了，因为任何人都可以针对远程主机建立中间人攻击/服务器。注意，这个插件不检查结束于非自签名证书中的证书链，而是由无法识别的证书颁发机构签名的证书链。 | | | | | |
| **加固建议：**为此服务购买或生成适当的证书。 | | | | | |
| Medium | 不需要 SMB 签名 |  | 5.0 | tcp | 445 |
| **漏洞描述：**远程 SMB 服务器上不需要签名。未经身份验证的远程攻击者可以利用这一点对 SMB 服务器进行中间人攻击。 | | | | | |
| **加固建议：**在主机配置中强制消息签名。在 Windows 上，这可以在策略设置“ Microsoft 网络服务器: 数字签名通信(总是)”中找到。在 Samba 上，这个设置称为“服务器签名”。详细信息请参阅“请参阅”链接。 | | | | | |
| Medium | 支持 SSL RC4密码套件(Bar Mitzvah) | CVE-2013-2566 | 4.3 | tcp | 3389 |
| **漏洞描述：**远程主机支持在一个或多个密码套件中使用 RC4。RC4密码在生成伪随机字节流方面存在缺陷，因此在字节流中引入了各种各样的小偏差，从而降低了其随机性。如果明文是重复加密的(例如 HTTP cookies) ，而攻击者能够获得许多(例如，数以千万计)密文，则攻击者可以获得明文。 | | | | | |
| **加固建议：**如果可能，重新配置受影响的应用程序，以避免使用 RC4密码。考虑在浏览器和 web 服务器支持的条件下使用带有 AES-GCM 套件的 TLS 1.2。 | | | | | |
| Medium | 支持 SSL RC4密码套件(Bar Mitzvah) | CVE-2015-2808 | 4.3 | tcp | 3389 |
| **漏洞描述：**远程主机支持在一个或多个密码套件中使用 RC4。RC4密码在生成伪随机字节流方面存在缺陷，因此在字节流中引入了各种各样的小偏差，从而降低了其随机性。如果明文是重复加密的(例如 HTTP cookies) ，而攻击者能够获得许多(例如，数以千万计)密文，则攻击者可以获得明文。 | | | | | |
| **加固建议：**如果可能，重新配置受影响的应用程序，以避免使用 RC4密码。考虑在浏览器和 web 服务器支持的条件下使用带有 AES-GCM 套件的 TLS 1.2。 | | | | | |
| Medium | MS16-047: SAM 和 LSAD 远程协议的安全更新(3148527)(Badlock)(未授权检查) | CVE-2016-0128 | 5.8 | tcp | 49161 |
| **漏洞描述：**由于远程过程调用(RPC)信道上的身份验证级别协商不当，安全帐户管理器(SAM)和本地安全权限(域策略)协议中的特权漏洞会增加，从而影响远程 Windows 主机。一个中间人攻击者能够拦截客户端和托管 SAM 数据库的服务器之间的通信，他可以利用这一点迫使认证级别降低，从而允许攻击者冒充一个经过认证的用户并访问 SAM 数据库。 | | | | | |
| **加固建议：**微软已经为 Windows Vista，2008,7,2008 r 2,2012,8.1，RT 8.1,2012 r 2和10发布了一系列补丁。 | | | | | |
| Medium | 1.0协议检测 |  | 6.1 | tcp | 3389 |
| **漏洞描述：**远程服务接受使用 TLS 1.0加密的连接。TLS 1.0有许多密码设计缺陷。TLS 1.0的现代实现缓解了这些问题，但是像1.2和1.3这样的 TLS 的新版本是针对这些缺陷设计的，应该尽可能地使用。截至2020年3月31日，不支持 TLS 1.2及以上版本的 Endpoints 在主流浏览器和主流厂商中将无法正常运行。PCI DSS v3.2要求在2018年6月30日之前完全禁用 TLS 1.0，但 POS POI 终端(以及它们连接的 SSL/TLS 终端点)可以被验证为不受任何已知漏洞的影响。 | | | | | |
| **加固建议：**启用对 TLS 1.2和1.3的支持，禁用对 TLS 1.0的支持。 | | | | | |
| Medium | 1.1协议检测 |  | 6.1 | tcp | 3389 |
| **漏洞描述：**远程服务接受使用 TLS 1.1加密的连接。TLS 1.1缺乏对当前和推荐的密码套件的支持。在 MAC 计算之前支持加密的加密器，以及认证加密模式，如 GCM 不能与 TLS 1.1一起使用。到2018年6月30日，PCI DSS v3.2仍然允许使用 TLS 1.1，但强烈建议使用 TLS 1.2。IETF 目前正在讨论一个完全不推荐 TLS 1.1的提议，许多供应商已经积极主动地这样做了。 | | | | | |
| **加固建议：**启用对 TLS 1.2和/或1.3的支持，并禁用 TLS 1.1的支持。 | | | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 信息 | 名称 | CVE | CVSS | protocol | port |
| Info | 服务器类型和版本 |  |  | tcp | 80 |
| **漏洞描述：**这个插件试图确定远程网络服务器的类型和版本。 | | | | | |
| Info | 服务器类型和版本 |  |  | tcp | 800 |
| **漏洞描述：**这个插件试图确定远程网络服务器的类型和版本。 | | | | | |
| Info | 服务器类型和版本 |  |  | tcp | 8080 |
| **漏洞描述：**这个插件试图确定远程网络服务器的类型和版本。 | | | | | |
| Info | 服务器类型和版本 |  |  | tcp | 8081 |
| **漏洞描述：**这个插件试图确定远程网络服务器的类型和版本。 | | | | | |
| Info | 服务器类型和版本 |  |  | tcp | 8083 |
| **漏洞描述：**这个插件试图确定远程网络服务器的类型和版本。 | | | | | |
| Info | 请求远程日期披露 | CVE-1999-0524 | 0.0 | icmp | 0 |
| **漏洞描述：**远程主机应答 ICMP 时间戳请求。这允许攻击者知道目标计算机上设置的日期，这可能有助于未经身份验证的远程攻击者击败基于时间的身份验证协议。从运行 Windows Vista/7/2008/2008 R2的计算机返回的时间戳故意不正确，但通常在实际系统时间的1000秒内。 | | | | | |
| **加固建议：**筛选出 ICMP 时间戳请求(13)和传出 ICMP 时间戳答复(14)。 | | | | | |
| Info | Windows NetBIOS/SMB 远程主机信息披露 |  |  | udp | 137 |
| **漏洞描述：**远程主机正在侦听 UDP 端口137或 TCP 端口445，并响应 NetBIOS nbtscan 或 SMB 请求。请注意，这个插件收集的信息将用于其他插件，但本身不生成报告。 | | | | | |
| Info | Traceroute Information |  |  | udp | 0 |
| **漏洞描述：**向远程主机生成一个 traceroute。 | | | | | |
| Info | DCE 服务枚举 |  |  | tcp | 135 |
| **漏洞描述：**通过向端口映射器(TCP 135或 epmapper PIPE)发送查找请求，可以枚举在远程端口上运行的分散式运算环境服务(DCE)。通过使用此信息，可以通过向远程端口/管道发送 RPC 请求来连接和绑定到每个服务。 | | | | | |
| Info | DCE 服务枚举 |  |  | tcp | 445 |
| **漏洞描述：**通过向端口映射器(TCP 135或 epmapper PIPE)发送查找请求，可以枚举在远程端口上运行的分散式运算环境服务(DCE)。通过使用此信息，可以通过向远程端口/管道发送 RPC 请求来连接和绑定到每个服务。 | | | | | |
| Info | DCE 服务枚举 |  |  | tcp | 49152 |
| **漏洞描述：**通过向端口映射器(TCP 135或 epmapper PIPE)发送查找请求，可以枚举在远程端口上运行的分散式运算环境服务(DCE)。通过使用此信息，可以通过向远程端口/管道发送 RPC 请求来连接和绑定到每个服务。 | | | | | |
| Info | DCE 服务枚举 |  |  | tcp | 49153 |
| **漏洞描述：**通过向端口映射器(TCP 135或 epmapper PIPE)发送查找请求，可以枚举在远程端口上运行的分散式运算环境服务(DCE)。通过使用此信息，可以通过向远程端口/管道发送 RPC 请求来连接和绑定到每个服务。 | | | | | |
| Info | DCE 服务枚举 |  |  | tcp | 49154 |
| **漏洞描述：**通过向端口映射器(TCP 135或 epmapper PIPE)发送查找请求，可以枚举在远程端口上运行的分散式运算环境服务(DCE)。通过使用此信息，可以通过向远程端口/管道发送 RPC 请求来连接和绑定到每个服务。 | | | | | |
| Info | DCE 服务枚举 |  |  | tcp | 49155 |
| **漏洞描述：**通过向端口映射器(TCP 135或 epmapper PIPE)发送查找请求，可以枚举在远程端口上运行的分散式运算环境服务(DCE)。通过使用此信息，可以通过向远程端口/管道发送 RPC 请求来连接和绑定到每个服务。 | | | | | |
| Info | DCE 服务枚举 |  |  | tcp | 49156 |
| **漏洞描述：**通过向端口映射器(TCP 135或 epmapper PIPE)发送查找请求，可以枚举在远程端口上运行的分散式运算环境服务(DCE)。通过使用此信息，可以通过向远程端口/管道发送 RPC 请求来连接和绑定到每个服务。 | | | | | |
| Info | DCE 服务枚举 |  |  | tcp | 49161 |
| **漏洞描述：**通过向端口映射器(TCP 135或 epmapper PIPE)发送查找请求，可以枚举在远程端口上运行的分散式运算环境服务(DCE)。通过使用此信息，可以通过向远程端口/管道发送 RPC 请求来连接和绑定到每个服务。 | | | | | |
| Info | 远程系统信息披露 |  |  | tcp | 445 |
| **漏洞描述：**Nessus 能够通过向端口139或445发送身份验证请求来获得远程操作系统名称和版本(Windows 和/或 Samba)。注意，这个插件要求在主机上启用 SMB1。 | | | | | |
| Info | SSL 证书信息 |  |  | tcp | 3389 |
| **漏洞描述：**这个插件连接到每个 ssl 相关的端口，并尝试提取和转储 x. 509证书。 | | | | | |
| Info | 启用 Windows 终端服务 |  |  | tcp | 3389 |
| **漏洞描述：**终端服务允许 Windows 用户远程获得图形登录(因此作为远程主机上的本地用户)。如果攻击者获得了有效的登录名和密码，则可以使用此服务进一步访问远程主机。攻击者也可以使用这个服务向远程主机挂载一个字典式攻击文件夹来尝试远程登录。注意，RDP (远程桌面协议)容易受到中间人攻击，这使得攻击者很容易通过模拟 Windows 服务器窃取合法用户的证书。 | | | | | |
| **加固建议：**如果您不使用终端服务，请禁用该服务，并且不允许该服务在 Internet 上运行。 | | | | | |
| Info | 微软 Windows SMB 服务检测 |  |  | tcp | 139 |
| **漏洞描述：**远程服务理解 CIFS (公共互联网文件系统)或服务器消息块(SMB)协议，用于在网络节点之间提供对文件、打印机等的共享访问。 | | | | | |
| Info | 微软 Windows SMB 服务检测 |  |  | tcp | 445 |
| **漏洞描述：**远程服务理解 CIFS (公共互联网文件系统)或服务器消息块(SMB)协议，用于在网络节点之间提供对文件、打印机等的共享访问。 | | | | | |
| Info | Nessus SYN 扫描器 |  |  | tcp | 80 |
| **漏洞描述：**这个插件是一个 SYN’半开’端口扫描器。即使对付一个有防火墙的目标，它也应该相当迅速。请注意，SYN 扫描比 TCP (完全连接)扫描破坏的服务的干扰性要小，但是如果网络已经加载，SYN 扫描可能会对不那么健壮的防火墙造成问题，并且在远程目标上留下未关闭的连接。 | | | | | |
| **加固建议：**用 IP 过滤器保护你的目标。 | | | | | |
| Info | Nessus SYN 扫描器 |  |  | tcp | 135 |
| **漏洞描述：**这个插件是一个 SYN’半开’端口扫描器。即使对付一个有防火墙的目标，它也应该相当迅速。请注意，SYN 扫描比 TCP (完全连接)扫描破坏的服务的干扰性要小，但是如果网络已经加载，SYN 扫描可能会对不那么健壮的防火墙造成问题，并且在远程目标上留下未关闭的连接。 | | | | | |
| **加固建议：**用 IP 过滤器保护你的目标。 | | | | | |
| Info | Nessus SYN 扫描器 |  |  | tcp | 139 |
| **漏洞描述：**这个插件是一个 SYN’半开’端口扫描器。即使对付一个有防火墙的目标，它也应该相当迅速。请注意，SYN 扫描比 TCP (完全连接)扫描破坏的服务的干扰性要小，但是如果网络已经加载，SYN 扫描可能会对不那么健壮的防火墙造成问题，并且在远程目标上留下未关闭的连接。 | | | | | |
| **加固建议：**用 IP 过滤器保护你的目标。 | | | | | |
| Info | Nessus SYN 扫描器 |  |  | tcp | 445 |
| **漏洞描述：**这个插件是一个 SYN’半开’端口扫描器。即使对付一个有防火墙的目标，它也应该相当迅速。请注意，SYN 扫描比 TCP (完全连接)扫描破坏的服务的干扰性要小，但是如果网络已经加载，SYN 扫描可能会对不那么健壮的防火墙造成问题，并且在远程目标上留下未关闭的连接。 | | | | | |
| **加固建议：**用 IP 过滤器保护你的目标。 | | | | | |
| Info | Nessus SYN 扫描器 |  |  | tcp | 800 |
| **漏洞描述：**这个插件是一个 SYN’半开’端口扫描器。即使对付一个有防火墙的目标，它也应该相当迅速。请注意，SYN 扫描比 TCP (完全连接)扫描破坏的服务的干扰性要小，但是如果网络已经加载，SYN 扫描可能会对不那么健壮的防火墙造成问题，并且在远程目标上留下未关闭的连接。 | | | | | |
| **加固建议：**用 IP 过滤器保护你的目标。 | | | | | |
| Info | Nessus SYN 扫描器 |  |  | tcp | 3389 |
| **漏洞描述：**这个插件是一个 SYN’半开’端口扫描器。即使对付一个有防火墙的目标，它也应该相当迅速。请注意，SYN 扫描比 TCP (完全连接)扫描破坏的服务的干扰性要小，但是如果网络已经加载，SYN 扫描可能会对不那么健壮的防火墙造成问题，并且在远程目标上留下未关闭的连接。 | | | | | |
| **加固建议：**用 IP 过滤器保护你的目标。 | | | | | |
| Info | Nessus SYN 扫描器 |  |  | tcp | 8080 |
| **漏洞描述：**这个插件是一个 SYN’半开’端口扫描器。即使对付一个有防火墙的目标，它也应该相当迅速。请注意，SYN 扫描比 TCP (完全连接)扫描破坏的服务的干扰性要小，但是如果网络已经加载，SYN 扫描可能会对不那么健壮的防火墙造成问题，并且在远程目标上留下未关闭的连接。 | | | | | |
| **加固建议：**用 IP 过滤器保护你的目标。 | | | | | |
| Info | Nessus SYN 扫描器 |  |  | tcp | 8081 |
| **漏洞描述：**这个插件是一个 SYN’半开’端口扫描器。即使对付一个有防火墙的目标，它也应该相当迅速。请注意，SYN 扫描比 TCP (完全连接)扫描破坏的服务的干扰性要小，但是如果网络已经加载，SYN 扫描可能会对不那么健壮的防火墙造成问题，并且在远程目标上留下未关闭的连接。 | | | | | |
| **加固建议：**用 IP 过滤器保护你的目标。 | | | | | |
| Info | Nessus SYN 扫描器 |  |  | tcp | 8083 |
| **漏洞描述：**这个插件是一个 SYN’半开’端口扫描器。即使对付一个有防火墙的目标，它也应该相当迅速。请注意，SYN 扫描比 TCP (完全连接)扫描破坏的服务的干扰性要小，但是如果网络已经加载，SYN 扫描可能会对不那么健壮的防火墙造成问题，并且在远程目标上留下未关闭的连接。 | | | | | |
| **加固建议：**用 IP 过滤器保护你的目标。 | | | | | |
| Info | 操作系统识别 |  |  | tcp | 0 |
| **漏洞描述：**使用远程探测的组合(例如，TCP/IP、 SMB、 HTTP、 NTP、 SNMP 等) ，可以猜测正在使用的远程操作系统的名称。有时也可以猜测操作系统的版本。 | | | | | |
| Info | Nessus 扫描信息 |  |  | tcp | 0 |
| **漏洞描述：**这个插件显示，对于每个被测试的主机，扫描本身的信息:-插件集的版本。- 扫描器的类型(Nessus 或 Nessus Home)。Nessus 引擎的版本。- 使用的端口扫描器。- 扫描的端口范围。- 是否可以进行授权或第三方补丁管理检查。- 扫描日期。- 扫描时间。- 同时扫描的主机数目。- 同时进行的检查次数。 | | | | | |
| Info | 虚拟机检测 |  |  | tcp | 0 |
| **漏洞描述：**根据其网络适配器的 MAC 地址，远程主机是一个 VMware 虚拟机。 | | | | | |
| **加固建议：**由于可以通过网络在物理上访问它，因此要确保其配置与组织的安全策略相匹配。 | | | | | |
| Info | 支持 SSL 密码组合 |  |  | tcp | 3389 |
| **漏洞描述：**此插件检测远程服务支持哪些 SSL 加密器来加密通信。 | | | | | |
| Info | 服务侦测 |  |  | tcp | 80 |
| **漏洞描述：**Nessus 能够通过其旗帜或者在接收到 HTTP 请求时查看其发送的错误消息来识别远程服务。 | | | | | |
| Info | 服务侦测 |  |  | tcp | 800 |
| **漏洞描述：**Nessus 能够通过其旗帜或者在接收到 HTTP 请求时查看其发送的错误消息来识别远程服务。 | | | | | |
| Info | 服务侦测 |  |  | tcp | 8080 |
| **漏洞描述：**Nessus 能够通过其旗帜或者在接收到 HTTP 请求时查看其发送的错误消息来识别远程服务。 | | | | | |
| Info | 服务侦测 |  |  | tcp | 8081 |
| **漏洞描述：**Nessus 能够通过其旗帜或者在接收到 HTTP 请求时查看其发送的错误消息来识别远程服务。 | | | | | |
| Info | 服务侦测 |  |  | tcp | 8083 |
| **漏洞描述：**Nessus 能够通过其旗帜或者在接收到 HTTP 请求时查看其发送的错误消息来识别远程服务。 | | | | | |
| Info | 超文本传输协议信息 |  |  | tcp | 80 |
| **漏洞描述：**这个测试提供了一些关于远程 HTTP 协议的信息——使用的版本，是否启用了 HTTP Keep-Alive 和 HTTP 管道等等。.这个测试只是信息性的，并不表示任何安全问题。 | | | | | |
| Info | 超文本传输协议信息 |  |  | tcp | 800 |
| **漏洞描述：**这个测试提供了一些关于远程 HTTP 协议的信息——使用的版本，是否启用了 HTTP Keep-Alive 和 HTTP 管道等等。.这个测试只是信息性的，并不表示任何安全问题。 | | | | | |
| Info | 超文本传输协议信息 |  |  | tcp | 8080 |
| **漏洞描述：**这个测试提供了一些关于远程 HTTP 协议的信息——使用的版本，是否启用了 HTTP Keep-Alive 和 HTTP 管道等等。.这个测试只是信息性的，并不表示任何安全问题。 | | | | | |
| Info | 超文本传输协议信息 |  |  | tcp | 8081 |
| **漏洞描述：**这个测试提供了一些关于远程 HTTP 协议的信息——使用的版本，是否启用了 HTTP Keep-Alive 和 HTTP 管道等等。.这个测试只是信息性的，并不表示任何安全问题。 | | | | | |
| Info | 超文本传输协议信息 |  |  | tcp | 8083 |
| **漏洞描述：**这个测试提供了一些关于远程 HTTP 协议的信息——使用的版本，是否启用了 HTTP Keep-Alive 和 HTTP 管道等等。.这个测试只是信息性的，并不表示任何安全问题。 | | | | | |
| Info | 支持 TCP/IP 时间戳 |  |  | tcp | 0 |
| **漏洞描述：**远程主机实现 TCP 时间戳，如 RFC1323所定义的。这个特性的一个副作用是，有时可以计算远程主机的正常运行时间。 | | | | | |
| Info | 以太网卡制造商检测 |  |  | tcp | 0 |
| **漏洞描述：**每个以太网 MAC 地址都以一个24位组织唯一标识符开头。 | | | | | |
| Info | Apache Tomcat 检测 |  |  | tcp | 8080 |
| **漏洞描述：**Nessus 能够检测到远程 Apache Tomcat web 服务器。 | | | | | |
| Info | HTTP 方法允许(每个目录) |  |  | tcp | 8083 |
| **漏洞描述：**通过调用 OPTIONS 方法，可以确定每个目录上允许使用哪些 HTTP 方法。下面的 HTTP 方法被认为是不安全的: PUT、 DELETE、 CONNECT、 TRACE、 HEAD 许多框架和语言将‘ HEAD’视为‘ GET’请求，尽管响应中没有任何主体。如果在“ GET”请求上设置了安全约束，只有“ authenticatedUsers”可以访问特定 servlet 或资源的 GET 请求，那么“ HEAD”版本将绕过该约束。这允许未经授权的盲目提交任何特权 GET 请求。由于这个列表可能不完整，插件还会测试每个目录上的各种已知 HTTP 方法，如果接收到的响应代码为400、403、405或501，插件还会测试是否启用了“彻底测试”或“启用 web 应用程序测试”在扫描策略中设置为“是”，并认为这些方法不受支持。注意，插件的输出只是信息性的，并不一定表明存在任何安全漏洞。 | | | | | |
| Info | 多 IP 地址枚举 |  |  | udp | 137 |
| **漏洞描述：**通过发送一个特殊的 NetBIOS 查询，Nessus 能够检测远程主机上多个 IP 地址的使用。这表明主机可能正在运行虚拟化软件、 VPN 客户端或具有多个网络接口。 | | | | | |
| Info | 公共平台枚举(CPE) |  |  | tcp | 0 |
| **漏洞描述：**通过使用从 Nessus 扫描获得的信息，这个插件报告 CPE (公共平台枚举)匹配主机上的各种硬件和软件产品。注意，如果产品没有官方的 CPE，这个插件会根据扫描得到的信息计算出最好的 CPE。 | | | | | |
| Info | 支持 SSL 会话恢复 |  |  | tcp | 3389 |
| **漏洞描述：**此脚本通过执行完整的 SSL 握手来检测主机是否允许恢复 SSL 会话，以接收会话 ID，然后重新连接到以前使用的会话 ID。如果服务器在第二个连接中接受会话 ID，则服务器维护一个会话缓存，可以继续进行。 | | | | | |
| Info | 设备类型 |  |  | tcp | 0 |
| **漏洞描述：**基于远程操作系统，可以确定远程系统类型(例如: 打印机、路由器、通用计算机等)。 | | | | | |
| Info | 支持 SSL/TLS 版本 |  |  | tcp | 3389 |
| **漏洞描述：**此插件检测哪些 SSL 和 TLS 版本支持远程服务，以便对通信进行加密。 | | | | | |
| Info | 支持 SSL/完备的前向安全性/密码套件 |  |  | tcp | 3389 |
| **漏洞描述：**远程主机支持使用 SSL 加密器，提供完备的前向安全性加密(PFS)。这些密码组合确保如果服务器的私钥受到破坏，那么在将来的某个日期，记录的 SSL 通信不会被破坏。 | | | | | |
| Info | 使用 SSL/TLS 的终端服务 |  |  | tcp | 3389 |
| **漏洞描述：**远程终端服务配置为使用 SSL/TLS。 | | | | | |
| Info | 支持 SSL 密码块链接密码套件 |  |  | tcp | 3389 |
| **漏洞描述：**远程主机支持使用在 Cipher Block Chaining (CBC)模式下运行的 SSL 加密程序。这些密码套件比电子密码本(Electronic Codebook，ECB)模式提供了额外的安全性，但如果使用不当，则有可能泄露信息。 | | | | | |
| Info | 以太网 MAC 地址 |  |  | tcp | 0 |
| **漏洞描述：**这个插件收集从主机的远程探测(例如 SNMP 和 Netbios)和运行本地检查(例如 ifconfig)中发现的 MAC 地址。然后，它将 MAC 地址合并成一个单一的、唯一的和统一的列表。 | | | | | |
| Info | 服务器消息块(SMB)协议版本1已启用(未授权的检查) |  |  | tcp | 445 |
| **漏洞描述：**远程 Windows 主机支持服务器消息块协议版本1(SMBv1)。微软建议用户停止使用 SMBv1，因为后来的 SMB 版本中缺乏安全特性。此外，据报道影子经纪人组有一个漏洞会影响 SMB; 然而，这个漏洞是否会影响 SMBv1或其他版本尚不清楚。针对这个问题，US-CERT 建议用户禁用 SMBv1/SMB 最佳实践，以缓解这些潜在问题。 | | | | | |
| **加固建议：**根据 Microsoft KB2696547中的供应商指令禁用 SMBv1。此外，通过阻塞所有网络边界设备上的 TCP 端口445，直接阻塞 SMB。对于基于 NetBIOS API 的 SMB，在所有网络边界设备上阻止 TCP 端口137/139和 UDP 端口137/138。 | | | | | |
| Info | 支持 microsoftwindows SMB 版本(远程检查) |  |  | tcp | 445 |
| **漏洞描述：**Nessus 能够通过向端口139或445发送身份验证请求来获得在远程主机上运行的 SMB 版本。注意，这个插件是一个远程检查，不能在代理上工作。 | | | | | |
| Info | 检测 |  |  | tcp | 80 |
| **漏洞描述：**Nessus 能够在远程主机上检测 JQuery。 | | | | | |
| Info | 支持 Microsoft Windows SMB2和 SMB3方言(远程检查) |  |  | tcp | 445 |
| **漏洞描述：**Nessus 可以通过向端口139或445发送一个身份验证请求来获得运行在远程主机上的 SMB2和 SMB3方言集。 | | | | | |
| Info | 没有提供证书 |  |  | tcp | 0 |
| **漏洞描述：**Nessus 无法执行凭证检查，因为没有提供凭证。 | | | | | |
| Info | 转储错误 |  |  | tcp | 0 |
| **漏洞描述：**这个插件解析 nessusd.dump 日志文件中的信息并报告错误。 | | | | | |
| Info | 本地检查未启用(信息) |  |  | tcp | 0 |
| **漏洞描述：**Nessus 没有在远程主机上启用本地检查。这并不一定表明扫描有问题。可能没有提供凭证，可能无法为目标提供本地检查，可能没有识别目标，或者可能发生了另一个问题，阻止启用本地检查。详细信息请参阅插件输出。此插件报告与未启用本地检查有关的信息检查结果。有关失败信息，请参见插件21745: “身份验证失败-本地检查未运行”。 | | | | | |