

|  |  |
| --- | --- |
| 文档编号 | AH-XXKH-0320 |
| 版本编号 | V1.0 |
| 密级 | 受控 |
| 日期 | 2023-03-20 |

|  |
| --- |
| XX客户  主机扫描报告 |

|  |
| --- |
| **©2021安恒信息** |
| **版权所有，未经授权，严禁复制、编辑和传播** |

* 适用性声明

本文档仅适用于杭州安恒信息技术股份有限公司（以下简称“安恒信息”）在XX客户（以下简称“XX客户”）开展主机扫描时的状况。主机扫描结束之后，因内部环境或不可预知的国内国际政治、经济、法律等社会环境的变化，可能会影响文档的有效性。再者，任何控制系统都存在固有的局限性，错误、违反内部控制的情况仍然有可能发生及不被发现。

* 版权声明

本文中的所有信息均为XX客户（以下简称“XX客户”）内部信息，务请妥善保管，未经XX客户和安恒信息明确作出的书面许可，不得为任何目的、以任何形式或手段（包括电子、机械、复印、录音或其他形式）对本文档的任何部分进行复制、存储、引入检索系统或者传播。

* 版本变更记录

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **版本号** | **拟制／修改日期** | **拟制／修改人** | **修改记录** | **批准人** |
| V0.1 | 2020-04-27 | 张韵 | 创建文档，添加样式库 | 韦国文 |
| V0.2 | 2020-07-30 | 甘雁南、苏启波 | 添加样式库、修改图注 | 韦国文 |
| V0.3 | 2020-09-08 | 甘雁南 | 修改格式和字体 | 韦国文 |
| V0.4 | 2020-10-23 | 王琦 | 修改格式 | 韦国文 |
| V1.0 | 2021-01-25 | 甄杰 | 修改格式和样式库 | 韦国文 |

目录

[一. 概述 3](#_Toc69344326)

[1.1 项目目标 3](#_Toc69344327)

[1.2 测试依据 3](#_Toc69344328)

[1.3 项目收益 3](#_Toc69344329)

[二. 实施范围 4](#_Toc69344330)

[三. 风险规避与处理措施 4](#_Toc69344331)

[3.1 风险规避措施 4](#_Toc69344332)

[3.1.1 系统备份与恢复 4](#_Toc69344333)

[3.1.2 风险与应对 4](#_Toc69344334)

[3.2 风险处理措施 4](#_Toc69344335)

[四. 检测结果与建议 5](#_Toc69344336)

1. 概述
   1. 项目目标

根据XX客户的安全性需求，授权杭州安恒信息技术股份有限公司（以下简称“安恒信息”）对其进行主机扫描测试；并根据本次扫描过程中所发现的系统脆弱点提供改进方案，以指导XX客户开展安全整改、完善安全策略，降低安全风险，使XX客户的安全保障能力符合国家的相关政策法规和自身业务的安全需求。

* 1. 测试依据

项目所依据及参考的标准：

《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）

《信息安全技术 信息安全风险评估规范》（GB/T 20984-2007）

《信息技术 安全技术 信息技术安全性评估准则》（GB/T 18336-2015）

《信息系统安全保障评估框架》（GB/T 20274-2006）

《OWASP测试指南V4.0》（2014）

《开源安全测试方法手册（OSSTMM）3》（2010）

《PTES渗透测试执行标准》（2011）

* 1. 项目收益

从攻击者的角度进行测试将有助于发现并识别出一些隐性存在的安全漏洞和风险点。

从客户收益的角度来说，可以对信息系统的安全性得到较深的感性认知，有助于后续的安全建设，对设备的版本、典型的可利用漏洞可以进行全面的排查，同时也可以用于验证经过安全保护后的网络是否真实的达到了预定安全目标、遵循了安全策略。

1. 实施范围

经过与XX客户协商确定，将主机扫描的时间安排为2023-03-20，主机扫描限定于以下对象：

|  |  |  |
| --- | --- | --- |
| 序号 | 测试对象 | 对象名称 |
| 1 | 10.36.211.160 | 温州公安 |
| 2 | 10.36.245.36 | 温州公安 |
| 3 | 10.36.245.48 | 温州公安 |
| 4 | 10.36.198.41 | 温州公安 |
| 5 | 10.36.208.40 | 温州公安 |
| 6 | 10.36.211.5 | 温州公安 |
| 7 | 10.36.198.38 | 温州公安 |
| 8 | 10.36.207.235 | 温州公安 |

1. 风险规避与处理措施
   1. 风险规避措施
      1. 系统备份与恢复

为防止在加固过程中出现的异常情况，所有被加固系统均应在被加固之前进行完整的系统备份,以便在系统发生灾难后及时恢复。

操作系统类：对系统的配置、用户目录和重要文件进行备份。例如：注册表、sam文件、/etc中的配置文件。并应该确保备份的自身安全。

数据库系统类：对数据库系统进行数据转储，并妥善保护好备份数据。同时对数据库系统的配置信息和用户信息进行备份。

网络应用系统类：对网络应用服务系统及其配置、用户信息、数据库等进行备份。

网络设备类：对网络设备的配置文件进行备份。

* + 1. 风险与应对

加固时间尽量安排在业务量不大的时段。在加固过程中如果出现被加固系统没有响应的情况，应立即停止加固工作，与配合人员一起分析情况，在确定原因后，并正确恢复系统，采取必要的预防措施后，才可以继续进行。

* 1. 风险处理措施

对信息系统安全加固过程中发现的风险，其处理方式一般有以下处理方式：

* 避免：指通过不继续进行可能产生风险的活动来避免风险。这种方式是最佳的解决方式，但实施的前提是要具有可行性，需要结合具体的实际情况在分析后决定。
* 转移：是指将相关的风险借助合同、保险以及合伙，合资等方式全部或部分转移给第三方，但这种转移一般只能降低部分经济损失或转移部分责任，不能降低安全本身的风险。
* 降低：通过采取相应的风险控制措施、安全机制来切实降低风险，减少发生的机率可能性，这也是采用最多的一种方式之一。
* 接受：在风险降低或转移后，可能还有剩余的风险，完全的零风险最理论和实践中都是不可能的，而且降低风险的成本会随着风险的降低而增大，通常考虑的尺度是让风险的处理成本与该项处理活动保持一种可接受的平衡。

1. 检测结果与建议

经过此次检测，共发现安全漏洞主机1个，其中紧急主机1个、高危主机0个、中危主机0个、低危主机0个。存在的安全隐患主要包括HTTP TRACE / TRAC方法未禁用、Web服务器info.php/phpinfo.php检测、Web服务器传输明文凭证等安全漏洞，可能将导致等严重危害。

* 1. 【紧急】（192.168.31.187）
     1. 【紧急】当前PHP版本厂商已不支持
* 漏洞描述：

根据现有版本，远程主机安装的PHP版本不再被厂商支持，意味着不再发布相关的安全补丁包，结果可能存在多个安全漏洞。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 192.168.31.187 | 8090 |

* 加固建议：

升级至当前的支持版本 http://php.net/eol.php https://wiki.php.net/rfc/releaseprocess

* + 1. 【紧急】Apache 2.2.x < 2.2.33-dev / 2.4.x < 2.4.26 多个漏洞
* 漏洞描述：

此版本受到以下漏洞影响： - httpd中存在身份验证绕过漏洞 由于第三方模块使用 ap\_get\_basic\_auth\_pw（）函数之外 验证阶段。远程攻击者可以利用此来绕过身份验证 要求。 （CVE-2017-3167） - httpd由于存在拒绝服务漏洞 一个NULL指针解除引用的缺陷，当 第三方模块调用mod\_ssl 一个HTTP期间的ap\_hook\_process\_connection（）函数 请求HTTPS端口。远程攻击者可以利用这一点导致拒绝服务 条件。 （CVE-2017-3169） - httpd由于存在拒绝服务漏洞 ap\_find\_token（）中的out-of-bounds读取错误 在特殊处理时触发的功能 制作的请求头序列。 远程攻击者可以利用这个来破坏它 服务或强制ap\_find\_token（）返回一个不正确的 值。 （CVE-2017-7668） - httpd由于存在拒绝服务漏洞 mod\_mime中出现超出范围的读取错误 在处理特制Content-Type时触发 响应头。远程攻击者可以 利用这一点来披露敏感信息或原因 拒绝服务条件。 （CVE-2017-7679） - httpd由于存在拒绝服务漏洞 无法初始化或重置值占位符 在[代理 - ]授权标题类型'Digest'之前 或在连续的键=值分配之间 mod\_auth\_digest的。远程攻击者可以 利用这个，通过提供没有'='的初始密钥 转让，披露敏感信息或导致 拒绝服务条件。 （CVE-2017-9788）

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 192.168.31.187 | 8090 |

* 加固建议：

升级Apache版本至2.2.33-dev / 2.4.26或之后的版本

* + 1. 【紧急】Apache 2.4.x <2.4.27多个漏洞
* 漏洞描述：

远程Web服务器受多个漏洞的影响

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 192.168.31.187 | 8090 |

* 加固建议：

升级到Apache版本2.4.27或更高版本

* + 1. 【紧急】Apache httpd 安全漏洞
* 漏洞描述：

Apache httpd 2.0.23版本至2.0.65版本、2.2.0版本至2.2.34和2.4.0版本至2.4.29版本中的mod\_authnz\_ldap存在安全漏洞。攻击者可利用该漏洞造成拒绝服务（崩溃和越边界写入）。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 192.168.31.187 | 8090 |

* 加固建议：

目前厂商已发布升级补丁以修复漏洞，补丁获取链接： https://httpd.apache.org/security/vulnerabilities\_24.html

* + 1. 【紧急】HTTP/2 资源管理错误漏洞
* 漏洞描述：

HTTP/2中存在资源管理错误漏洞。攻击者可利用该漏洞导致拒绝服务。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 192.168.31.187 | 8090 |

* 加固建议：

厂商已发布升级补丁以修复漏洞，详情请关注厂商主页： https://http2.github.io/

* + 1. 【紧急】Apache 2.4.x<2.4.46多个漏洞
* 漏洞描述：

安装在远程主机上的Apache httpd版本早于2.4.46。因此，它受到2.4.46建议中提到的多个漏洞的影响Apache HTTP server 2.4.32至2.4.44 mod\_proxy\_uwsgi info disclosure and possible RCE（CVE-2020-11984）-Apache HTTP server版本2.4.20至2.4.43当对HTTP/2模块和某些流量边缘模式启用跟踪/调试时，在错误连接上执行日志语句，导致内存池的并发使用。配置mod\_http2的LogLevel over info将缓解未修补服务器的此漏洞(CVE-2020-11993）-Apache HTTP服务器版本2.4.20至2.4.43。在HTTP/2请求中，为“Cache Digest”头精心编制的值将导致在服务器实际尝试HTTP/2之后推送资源时崩溃。通过H2Push-off配置HTTP/2功能将缓解未修补服务器的此漏洞(（CVE-2020-9490）请注意，Nessus尚未对此问题进行测试，而是仅依赖于应用程序的自我报告版本号。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 192.168.31.187 | 8090 |

* 加固建议：

升级至Apache 2.4.46或更高版本。

* + 1. 【紧急】Apache 2.4。x<2.4.47多个漏洞
* 漏洞描述：

远程主机上安装的Apache httpd版本早于2.4.47。因此，它受到2.4.47变更日志中引用的多个漏洞的影响：-与“MergeSlashes OFF”（CVE-2021-30641）匹配的意外<Location>部分-mod\_auth\_digest:验证摘要nonce时，堆栈可能溢出一个nul字节。（CVE-2020-35452）-mod\_session：修复由于空指针解引用导致的可能崩溃，该故障可用于导致恶意后端服务器和SessionHeader的拒绝服务。（CVE-2021-26691）-mod\_会话：修复可能由于空指针解引用而导致的崩溃，这可能会导致拒绝服务。（CVE-2021-26690）-mod\_proxy\_http：修复可能因空指针解引用而导致的崩溃，该故障可用于导致拒绝服务。（CVE-2020-13950）-Windows：防止本地用户停止httpd进程（CVE-2020-13938）-mod\_proxy\_wstunnel，mod\_proxy\_http：处理可升级的协议端到端协商。（CVE-2019-17567）请注意，Nessus没有针对该问题进行测试，而是仅依赖于应用程序的自我报告版本号。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 192.168.31.187 | 8090 |

* 加固建议：

升级至Apache 2.4.47或更高版本。

* + 1. 【紧急】Apache<2.4.49多个漏洞
* 漏洞描述：

远程主机上安装的Apache httpd版本早于2.4.49。因此，它受到2.4.49变更日志中引用的漏洞的影响。-精心编制的请求uri路径可能会导致mod\_proxy将请求转发到远程用户选择的源服务器。（CVE-2021-40438）请注意，Nessus没有针对这个问题进行测试，而是只依赖于应用程序的自我报告版本号。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 192.168.31.187 | 8090 |

* 加固建议：

升级至Apache 2.4.49或更高版本。

* + 1. 【紧急】Apache<2.4.49多个漏洞
* 漏洞描述：

远程主机上安装的Apache httpd版本早于2.4.49。因此，它受到2.4.49变更日志中引用的多个漏洞的影响。-当给定恶意输入时，ap\_escape\_quotes（）可能会写入缓冲区之外的内容。没有包含的模块将不受信任的数据传递给这些功能，但第三方/外部模块可能会。（CVE-2021-39275）-格式错误的请求可能会导致服务器取消对空指针的引用。（CVE-2021-34798）请注意，Nessus没有针对该问题进行测试，而是仅依赖于应用程序的自我报告版本号。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 192.168.31.187 | 8090 |

* 加固建议：

升级至Apache 2.4.49或更高版本。

* + 1. 【紧急】Apache 2.4。x<2.4.52多个漏洞
* 漏洞描述：

远程主机上安装的Apache httpd版本早于2.4.52。因此，它受到2.4.52建议中提到的多个漏洞的影响。-发送到配置为转发代理（ProxyRequests on）的httpd的精心编制的URI可能会导致崩溃（空指针取消引用），或者，对于混合了转发和反向代理声明的配置，可以允许将请求定向到已声明的Unix域套接字端点（服务器端请求伪造）。此问题影响Apache HTTP服务器2.4.7至2.4.51（包括）。（CVE-2021-44224）-精心编制的请求正文可能会导致mod\_lua多部分解析器中的缓冲区溢出（从lua脚本调用r:parsebody（））。Apache httpd团队不知道有人利用该漏洞进行攻击，尽管可能会设计一个漏洞。此问题影响Apache HTTP Server 2.4.51及更早版本。（CVE-2021-44790）请注意，Nessus没有针对该问题进行测试，而是仅依赖于应用程序的自我报告版本号。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 192.168.31.187 | 8090 |

* 加固建议：

升级至Apache 2.4.52或更高版本。

* + 1. 【紧急】Apache 2.4.x<2.4.53多个漏洞
* 漏洞描述：

远程主机上安装的Apache httpd版本早于2.4.53。因此，它受到2.4.53咨询中提到的多个漏洞的影响mod\_lua在r:parsebody中使用未初始化的值：精心设计的请求体可能会导致对随机内存区域的读取，从而导致进程崩溃。此问题影响Apache HTTP Server 2.4.52和更早版本。确认：Chamal De Silva（CVE-2022-22719）-HTTP请求走私：当遇到错误时，Apache HTTP Server 2.4.52和更早版本无法关闭入站连接，丢弃请求主体，将服务器暴露于HTTP请求走私确认：James Kettle<James.kett portswigger.net>（CVE-2022-22720）-内核中可能存在非常大或无限的LimitXMLRequestBody缓冲区溢出：如果LimitXMLRequest Body设置为允许32位系统上的请求体大于350MB（默认值为1M），则会发生整数溢出，随后会导致越界写入。此问题影响Apache HTTP Server 2.4.52和更早版本。确认：匿名使用Trend Micro Zero Day Initiative（CVE-2022-22721）-mod\_sed中的读/写超出界限：Apache HTTP服务器mod\_sed的写漏洞允许攻击者使用攻击者提供的数据覆盖堆内存。此问题会影响Apache HTTP Server 2.4版本2.4.52和以前的版本。致谢：Ronald Crane（Zippenhop LLC）（CVE-2022-23943）请注意，Nessus尚未对此问题进行测试，而是仅依赖于应用程序的自报告版本号。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 192.168.31.187 | 8090 |

* 加固建议：

升级至Apache 2.4.53或更高版本。

* + 1. 【紧急】OpenSSL 1.0.2<1.0.2ze漏洞
* 漏洞描述：

远程主机上安装的OpenSSL版本早于1.0.2ze。因此，它受到1.0.2ze建议中提到的漏洞的影响。-c\_rehash脚本未正确清除shell元字符以防止命令注入。此脚本由某些操作系统以自动执行的方式分发。在这样的操作系统上，攻击者可以使用脚本的权限执行任意命令。c\_rehash脚本的使用被认为是过时的，应该用OpenSSL rehash命令行工具代替。已在OpenSSL 3.0.3中修复（受影响的3.0.0、3.0.1、3.0.2）。在OpenSSL 1.1.1o中修复（受到影响的1.1.1-1.1.1n）。在OpenSL 1.0.2ze中修复（被影响的1.0.2-1.0.2zd）。（CVE-2022-1292）请注意，Nessus尚未对此问题进行测试，而是仅依赖于应用程序的自报版本号。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 192.168.31.187 | 8090 |

* 加固建议：

升级至OpenSSL 1.0.2ze或更高版本。

* + 1. 【紧急】Apache 2.4.x<2.4.52 mod\_lua缓冲区溢出
* 漏洞描述：

远程主机上安装的Apache httpd版本早于2.4.52。因此，在处理多部分内容时，它受到与mod\_lua相关的缺陷的影响。精心制作的请求体可能会导致mod\_lua多部分解析器（从lua脚本调用的r:parsebody（））中的缓冲区溢出。Apache httpd团队没有意识到该漏洞的漏洞，尽管可能会精心设计一个漏洞。请注意，Nessus没有对此问题进行测试，而是仅依赖于应用程序的自报告版本号。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 192.168.31.187 | 8090 |

* 加固建议：

升级至Apache 2.4.52或更高版本。

* + 1. 【紧急】Apache 2.4.x<2.4.54多个漏洞
* 漏洞描述：

远程主机上安装的Apache httpd版本早于2.4.54。因此，它受到2.4.54咨询中提到的多个漏洞的影响mod\_proxy\_ajp中可能存在请求走私：Apache HTTP Server mod\_proxy-ajp中的HTTP请求解释不一致（“HTTP请求走私”）漏洞允许攻击者将请求走私到其转发请求的ajp服务器。此问题会影响Apache HTTP Server Apache HTTP Server 2.4 2.4.53版和更早版本。确认：Ricter Z@360 Noah Lab（CVE-2022-26377）-在mod\_isapi中读取超出界限：Windows上的Apache HTTP Server 2.4.53和更早版本在配置为使用mod\_isap模块处理请求时可能读取超出界限。致谢：Apache HTTP Server项目要感谢Ronald Crane（Zippenhop LLC）报告了此问题（CVE-2022-28330）-通过ap\_rwrite（）读取超出界限：如果攻击者可以使用ap\_rwrite（）或ap\_rputs（）导致服务器反映非常大的输入，Apache HTTP Server 2.4.53和更早版本中的ap\_rrite（）函数可能会读取非预期内存，例如使用mod\_luas r:puts（）函数。致谢：Apache HTTP Server项目要感谢Ronald Crane（Zippenhop LLC）报告了这个问题（CVE-2022-28614）-ap\_strcmp\_match（）中的读取超出界限：如果提供了非常大的输入缓冲区，Apache HTTP Server 2.4.53和更早版本可能会崩溃或泄露信息，因为ap\_strcmp\_match（（）中存在读取超出界限。虽然没有随服务器分发的代码可以强制执行这样的调用，但使用ap\_strcmp\_match（）的第三方模块或lua脚本可能会受到影响。致谢：Apache HTTP Server项目感谢Ronald Crane（Zippenhop LLC）报告了这个问题（CVE-2022-28615）——mod\_lua r:parsebody中的拒绝服务：在Apache HTTP Server 2.4.53和更早版本中，对调用r:parsebody（0）的lua脚本的恶意请求可能会导致拒绝服务，因为可能的输入大小没有默认限制。致谢：Apache HTTP Server项目要感谢Ronald Crane（Zippenhop LLC）报告了这个问题（CVE-2022-29404）-拒绝服务mod\_sed：如果Apache HTTP Server 2.4.53配置为在mod\_sed的输入可能非常大的上下文中使用mod\_sed进行转换，mod\_sed可能会进行过大的内存分配并触发中止。确认：此问题由JFrog安全研究团队（CVE-2022-30522）的Brian Moussalli发现-使用websockets:Apache HTTP Server 2.4.53和更早版本的mod\_lua中的信息泄漏可能会向调用r:wsread（）的应用程序返回超过为缓冲区分配的存储末尾的长度。致谢：Apache HTTP Server项目要感谢Ronald Crane（Zippenhop LLC）报告了此问题（CVE-2022-30556）-X-Forwarded-for mod\_proxy中逐跳丢弃机制：Apache HTTP服务器2.4.53和更早版本可能不会基于客户端连接头逐跳机制将X-Forwarded-\*头发送到源服务器。这可用于绕过源服务器/应用程序上基于IP的身份验证。致谢：Apache HTTP Server项目要感谢Gaetan Ferry（Synacktiv）报告了这个问题（CVE-2022-31813）。请注意，Nessus没有针对这些问题进行测试，而是仅依赖于应用程序的自我报告版本号。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 192.168.31.187 | 8090 |

* 加固建议：

升级至Apache 2.4.54或更高版本。

* + 1. 【紧急】OpenSSL 1.0.2<1.0.2zf漏洞
* 漏洞描述：

远程主机上安装的OpenSSL版本早于1.0.2zf。因此，它受到1.0.2zf建议中提到的漏洞的影响。请注意，Nessus没有对此问题进行测试，而是仅依赖于应用程序的自报告版本号。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 192.168.31.187 | 8090 |

* 加固建议：

升级至OpenSSL 1.0.2zf或更高版本。

* + 1. 【紧急】Apache 2.4.x<2.4.55多个漏洞
* 漏洞描述：

远程主机上安装的Apache httpd版本早于2.4.55。因此，它受到2.4.55咨询中提到的多个漏洞的影响精心制作的If：request标头可能会导致池（堆）内存位置中超出发送的标头值的单个零字节的内存读取或写入。这可能会导致进程崩溃。此问题影响Apache HTTP Server 2.4.54和更早版本。（CVE-2006-20001）-Apache HTTP Server mod\_proxy\_ajp中的HTTP请求解释不一致（“HTTP请求走私”）漏洞允许攻击者将请求走私到其转发请求的ajp服务器。此问题影响Apache HTTP Server Apache HTTP Server 2.4 2.4.54版及更早版本。（CVE-2022-36760）-在Apache HTTP Server 2.4.55之前，恶意后端可能会导致响应标头提前被截断，从而导致一些标头被合并到响应主体中。如果后面的标头有任何安全目的，客户端将不会解释它们。（CVE-2022-37436）请注意，Nessus没有针对这些问题进行测试，而是仅依赖于应用程序的自我报告版本号。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 192.168.31.187 | 8090 |

* 加固建议：

升级至Apache 2.4.55或更高版本。

* + 1. 【高危】Apache 2.4.x <2.4.25多个漏洞（httpoxy）
* 漏洞描述：

远程Web服务器受多个漏洞的影响

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 192.168.31.187 | 8090 |

* 加固建议：

升级到Apache版本2.4.25或更高版本

* + 1. 【高危】“Optionsbleed”-Apache HTTP OPTIONS方法内存泄露漏洞
* 漏洞描述：

2017年9月18日，Apache被爆存在高安全风险漏洞，漏洞CVE编号:CVE-2017-9798,该漏洞发现于Apache HTTP 软件 2.2.34/2.4.27版本，该漏洞Limit指令的函数ap\_limit\_section所触发，如果网站管理员尝试使用无效的 HTTP 方法进行 “Limit” 指令HTTP请求时，会导致内存信息泄露，目前该漏洞证明已经公开，存在安全风险。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 192.168.31.187 | 8090 |

* 加固建议：

建议升级到最新版本

* + 1. 【高危】Apache HTTP Server 资源管理错误漏洞
* 漏洞描述：

Apache HTTP Server中存在拒绝服务漏洞。远程攻击者可通过发送特制的HTTP/2请求利用该漏洞造成拒绝服务。以下版本受到影响：Apache HTTP Server 2.4.18版本，2.4.20版本，2.4.23版本，2.4.29版本，2.4.33版本，2.4.30版本。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 192.168.31.187 | 8090 |

* 加固建议：

目前厂商已发布升级补丁以修复漏洞，补丁获取链接: https://httpd.apache.org/security/vulnerabilities\_24.html

* + 1. 【高危】Apache HTTP Server 资源管理错误漏洞
* 漏洞描述：

Apache HTTP Server 2.4.17版本至2.4.37版本中存在资源管理错误漏洞。该漏洞源于网络系统或产品对系统资源（如内存、磁盘空间、文件等）的管理不当。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 192.168.31.187 | 8090 |

* 加固建议：

目前厂商已发布升级补丁以修复漏洞，补丁获取链接： https://httpd.apache.org/security/vulnerabilities\_24.html

* + 1. 【高危】Apache httpd 安全漏洞
* 漏洞描述：

Apache httpd 2.4.18版本至2.4.38版本中存在安全漏洞。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 192.168.31.187 | 8090 |

* 加固建议：

目前厂商已发布升级补丁以修复漏洞，补丁获取链接： https://httpd.apache.org/security/vulnerabilities\_24.html

* + 1. 【高危】PHP<7.3.24多个漏洞
* 漏洞描述：

根据其自报的版本号，在远程web服务器上运行的PHP版本早于7.3.24。因此，它受到多个漏洞的影响

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 192.168.31.187 | 8090 |

* 加固建议：

升级至PHP版本7.3.24或更高版本。

* + 1. 【高危】OpenSSL 1.0.2<1.0.2za漏洞
* 漏洞描述：

远程主机上安装的OpenSSL版本早于1.0.2za。因此，它受到1.0.2za建议中提到的漏洞的影响。-ASN。1字符串在OpenSSL内部表示为ASN1\_字符串结构，其中包含一个保存字符串数据的缓冲区和一个保存缓冲区长度的字段。这与普通的C字符串形成对比，后者作为字符串数据的缓冲区，以NUL（0）字节结尾。虽然不是严格的要求，ASN。1使用OpenSSL自己的d2i函数（和其他类似的解析函数）解析的字符串，以及使用ASN1\_string\_set（）函数设置值的任何字符串，将额外NUL终止ASN1\_字符串结构中的字节数组。但是，应用程序可以通过直接设置ASN1\_字符串数组中的数据和长度字段，直接构造有效的ASN1\_字符串结构，而不会以NUL终止字节数组。这也可以通过使用ASN1\_STRING\_set0（）函数实现。许多打印ASN的OpenSSL函数。1已发现数据假设ASN1\_字符串字节数组将以NUL结尾，尽管直接构造的字符串不能保证这一点。其中应用程序请求ASN。1要打印的结构，以及ASN的位置。1结构包含由应用程序直接构造的ASN1\_字符串，无需NUL终止数据字段，则可能发生读取缓冲区溢出。在证书的名称约束处理过程中也可能发生同样的情况（例如，如果证书是由应用程序直接构造的，而不是通过OpenSSL解析函数加载的，并且证书包含以非NUL结尾的ASN1\_字符串结构）。它也可以出现在X509\_get1\_email（）、X509\_REQ\_get1\_email（）和X509\_get1\_ocsp（）函数中。如果恶意参与者可以导致应用程序直接构造ASN1\_字符串，然后通过受影响的OpenSSL函数之一对其进行处理，那么这个问题可能会受到影响。这可能会导致崩溃（导致拒绝服务攻击）。它还可能导致私密内存内容（如私钥或敏感明文）的泄露。在OpenSSL 1.0.2za中修复（受影响1.0.2-1.0.2y）。（CVE-2021-3712）请注意，Nessus没有针对该问题进行测试，而是仅依赖于应用程序的自我报告版本号。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 192.168.31.187 | 8090 |

* 加固建议：

升级至OpenSSL 1.0.2za或更高版本。

* + 1. 【高危】Apache>=2.4.17<2.4.49 mod\_http2
* 漏洞描述：

安装在远程主机上的Apache httpd版本高于2.4.17，低于2.4.49。因此，它受到2.4.49变更日志中引用的漏洞的影响。通过HTTP/2发送的特制方法将绕过验证，并由mod\_代理转发，这可能会导致请求拆分或缓存中毒。请注意，Nessus没有针对这个问题进行测试，而是只依赖于应用程序的自我报告版本号。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 192.168.31.187 | 8090 |

* 加固建议：

升级至Apache 2.4.49或更高版本。

* + 1. 【高危】OpenSSL 1.0.2<1.0.2zd漏洞
* 漏洞描述：

远程主机上安装的OpenSSL版本早于1.0.2zd。因此，它受到1.0.2zd建议中提到的漏洞的影响。-计算模平方根的BN\_mod\_sqrt（）函数包含一个错误，它可能导致非素模永远循环。在内部，当解析包含压缩形式的椭圆曲线公钥或以压缩形式编码的基点的显式椭圆曲线参数的证书时，使用此函数。通过制作具有无效显式曲线参数的凭证，可以触发无限循环。由于证书解析发生在验证证书签名之前，因此解析外部提供的证书的任何进程都可能受到拒绝服务攻击。解析特制的私钥时也可以到达无限循环，因为它们可以包含显式椭圆曲线参数。因此，易受攻击的情况包括：-TLS客户端使用服务器证书-TLS服务器使用客户端证书-托管提供商从客户处获取证书或私钥-证书颁发机构解析来自订户的证书请求-解析ASN.1椭圆曲线参数的任何其他应用程序还有任何使用BN\_mod\_sqrt（）的应用程序，其中攻击者可以控制参数值，因此易受此DoS问题的影响。在OpenSSL 1.0.2版本中，公钥在证书的初始解析过程中不被解析，这使得触发无限循环稍微困难一些。然而，任何需要证书公钥的操作都将触发无限循环。特别是，攻击者可以在验证证书签名期间使用自签名证书来触发循环。此问题影响OpenSSL版本1.0.2、1.1.1和3.0。在2022年3月15日发布的1.1.1n和3.0.2版本中解决了这一问题。已在OpenSSL 3.0.2中修复（受影响的3.0.0,3.0.1）。已在OpenSSL1.1.1n中修复（受到影响的1.1.1-1.1.1m）。在OpenSSL 1.0.2zd中修复（被影响的1.0.2-1.0.2zc）。（CVE-2022-0778）请注意，Nessus尚未对此问题进行测试，而是仅依赖于应用程序的自报版本号。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 192.168.31.187 | 8090 |

* 加固建议：

升级至OpenSSL 1.0.2zd或更高版本。

* + 1. 【高危】OpenSSL 1.0.2<1.0.2zg多个漏洞
* 漏洞描述：

远程主机上安装的OpenSSL版本早于1.0.2zg。因此，它受到1.0.2zg建议中提到的多个漏洞的影响。-X.509 GeneralName中存在与X.400地址处理相关的类型混淆漏洞。X.400地址被解析为ASN1\_STRING，但GENERAL\_NAME的公共结构定义错误地将x400Address字段的类型指定为ASN1\_type。随后，OpenSSL函数GENERAL\_NAME\_cmp将此字段解释为ASN1\_TYPE，而不是ASN1\_STRING。启用CRL检查时（即应用程序设置X509\_V\_FLAG\_CRL\_CHECK标志），此漏洞可能允许攻击者向memcmp调用传递任意指针，使其能够读取内存内容或执行拒绝服务。在大多数情况下，攻击要求攻击者同时提供证书链和CRL，两者都不需要有效签名。如果攻击者只控制其中一个输入，则另一个输入必须已经包含X.400地址作为CRL分发点，这是不常见的。因此，此漏洞很可能只影响已实现自己的功能以通过网络检索CRL的应用程序。感谢David Benjamin（谷歌）。由Hugo Landau开发的Fix。已在OpenSSL 1.0.2zg中修复（自1.0.2起受影响）。（CVE-2023-0286）-公共API函数BIO\_new\_NDEF是用于通过BIO流式传输ASN.1数据的助手函数。它主要用于OpenSSL内部，以支持SMIME、CMS和PKCS7流式传输功能，但也可由最终用户应用程序直接调用。该函数从调用方接收BIO，在其前面准备一个新的BIO\_f\_asn1过滤器BIO以形成BIO链，然后将BIO链的新头返回给调用方。在某些情况下，例如，如果CMS接收方公钥无效，则释放新的筛选器BIO，函数返回NULL结果，表示失败。但是，在这种情况下，BIO链没有被正确清理，调用方传递的BIO仍然保留指向先前释放的筛选器BIO的内部指针。如果调用方随后继续在BIO上调用BIO\_pop（），则将发生释放后使用。这很可能导致撞车。这种情况直接发生在内部函数B64\_write\_ASN1（）中，这可能会导致BIO\_new\_NDEF（）被调用，随后将在BIO上调用BIO\_pop（）。该内部函数依次由公共API函数PEM\_write\_BIO\_ASN1\_stream、PEM\_write\_BIO\_CMS\_stream、PEM\_write\_BIO\_PKCS7\_stream，SMIME\_write\_ASN1、SMIME\_write\_CMS和SMIME\_white\_PKCS7调用。可能受此影响的其他公共API函数包括i2d\_ASN1\_bio\_stream、bio\_new\_CMS、bio\_news\_PKCS7、i2d\_CMS\_bio\_strea和i2d\_PKCS7\_bio\_stream。OpenSSL cms和smime命令行应用程序也受到类似的影响。感谢Octavio Galland（马克斯·普朗克安全与隐私研究所）。感谢Marcel Bhme（马克斯·普朗克安全与隐私研究所）。由Viktor Dukhovni开发的修复程序。修复由Matt Caswell开发。已在OpenSSL 1.0.2zg中修复（自1.0.2起受影响）。（CVE-2023-0215）-OpenSSL RSA解密实现中存在基于时间的侧信道，这足以在Bleichenbacher式攻击中恢复网络上的明文。为了成功解密，攻击者必须能够发送大量的尝试消息进行解密。该漏洞影响所有RSA填充模式：PKCS#1 v1.5、RSA-OEAP和RSASVE。例如，在TLS连接中，客户端通常使用RSA向服务器发送加密的预主密钥。观察到客户端和服务器之间存在真实连接的攻击者可以利用此漏洞向服务器发送试用消息，并记录处理这些消息所需的时间。在足够多的消息之后，攻击者可以恢复用于原始连接的预主密钥，从而能够解密通过该连接发送的应用程序数据。已在OpenSSL 1.0.2zg中修复（自1.0.2起受影响）。（CVE-2022-4304）请注意，Nessus没有针对这些问题进行测试，而是仅依赖于应用程序的自报告版本号。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 192.168.31.187 | 8090 |

* 加固建议：

升级至OpenSSL 1.0.2zg或更高版本。

* + 1. 【中危】HTTP TRACE / TRAC方法未禁用
* 漏洞描述：

主机支持TRACE和/或TRACK方法。 TRACE和TRACK是HTTP用来调试web服务器连接的方法。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 192.168.31.187 | 8090 |

* 加固建议：

禁用TRACE / TRAC方法，参考如下： 1、IIS下：IIS信息服务－web服务扩展：禁止"WebDAV； 2、apache下：修改httpd.conf配置文件中"TraceEnable on"为"TraceEnable off"

* + 1. 【中危】Web服务器info.php/phpinfo.php检测
* 漏洞描述：

许多PHP安装教程指导用户创建一个PHP文件，该文件调用PHP函数“phpinfo（）”进行调试。各种PHP应用程序也可能包含这样的文件。通过访问这样的文件，远程攻击者可以发现有关远程web服务器的大量信息，包括：-安装PHP的用户的用户名，如果他们是SUDO用户。-主机的IP地址。-操作系统的版本。-web服务器版本。-web服务器的根目录。-有关远程PHP安装的配置信息。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 192.168.31.187 | 8090 |

* 加固建议：

删除受影响的文件。

* + 1. 【中危】SSL证书主机名不匹配
* 漏洞描述：

SSL现有认证的commonName (CN)是供其它主机使用的。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 192.168.31.187 | 443 |

* 加固建议：

为此项服务购买或生产一个合适的证书

* + 1. 【中危】PHP expose.PHP信息泄漏
* 漏洞描述：

远程服务器上的PHP安装以允许通过特殊URL向攻击者泄露潜在敏感信息的方式进行配置。这样的URL会触发PHP本身内置的复活节彩蛋。其他类似的复活节彩蛋也可能存在，但奈索斯没有检查过。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 192.168.31.187 | 8090 |

* 加固建议：

在PHP配置文件PHP.ini中，将“expose.PHP”的值设置为“Off”以禁用此行为。重新启动web服务器守护程序以使此更改生效。

* + 1. 【中危】SSL证书不被信任
* 漏洞描述：

此项服务的SSL证书不被信任。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 192.168.31.187 | 443 |

* 加固建议：

为此项服务购买或生成合适的证书

* + 1. 【中危】SSL自签名证书
* 漏洞描述：

服务器所使用的X.509签署的证书链不是权威的证书颁发机构所颁发的。这削弱了使用SSL的效果，因为任何人都可以建立一个中间人攻击远程主机。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 192.168.31.187 | 443 |

* 加固建议：

购买或者生成被认可的证书

* + 1. 【中危】SMB数字签名通信禁用
* 漏洞描述：

SMB 协议为 Microsoft 文件和打印共享以及许多其他网络操作（例如远程 Windows 管理）提供基础。为了防止在传输过程中修改 SMB 数据包的拦截攻击，SMB 协议支持对 SMB 数据包的数字签名。 主机禁用了SMB数字签名通信，这可能导致潜在攻击者针对SMB通信服务进行中间人攻击。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 192.168.31.187 | 445 |

* 加固建议：

在本地策略中--安全选项设置如下： Microsoft 网络客户端：对通信进行数字签名（若服务器同意）（启用） Microsoft 网络服务器：对通信进行数字签名（若客户同意）（启用）

* + 1. 【中危】Web应用程序可能容易受到点击劫持
* 漏洞描述：

远程Web服务器不会在所有内容响应中设置X-Frame-Options响应标头或Content-Security-Policy“frame-ancestors”响应标头。这可能会使网站遭受点击劫持或UI补救攻击，攻击者可以欺骗用户点击与用户感知页面不同的易受攻击页面区域。这可能会导致用户进行欺诈或恶意交易。 微软已经提出X-Frame-Options作为缓解点击劫持攻击的一种方法，并且目前被所有主流浏览器厂商所支持。 W3C网络应用安全工作组已经提出了内容安全策略（CSP），并加强了所有主要浏览器厂商的支持，以此来缓解点击劫持和其他攻击。 “框架 - 祖先”政策指令限制哪些来源可以嵌入受保护的资源。 请注意，尽管X-Frame-Options和Content-Security-Policy响应头并不是clickjacking的唯一缓解措施，它们是目前最可靠的方法，可以通过自动化进行检测。因此，如果部署了其他缓解策略（例如，框架抽取JavaScript）或者页面不执行任何安全敏感的事务，该插件可能会产生误报。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 192.168.31.187 | 8090 |

* 加固建议：

返回带有页面响应的X-Frame-Options或Content-Security-Policy（带有“frame-ancestors”指令）HTTP头。 这可以防止使用框架或iframe HTML标记时页面内容被其他站点呈现。

* + 1. 【中危】OpenSSL 1.0.2 <1.0.2k多种漏洞
* 漏洞描述：

在远程主机上运行的服务受多个影响 漏洞

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 192.168.31.187 | 8090 |

* 加固建议：

升级到OpenSSL版本1.0.2k或更高版本。

* + 1. 【中危】OpenSSL安全功能绕过漏洞
* 漏洞描述：

OpenSSL 1.1.0、1.0.2版本解析X.509证书的畸形IPAddressFamily扩展时，存在单字节缓冲区溢出漏洞，可导致证书以文本格式显示时出现错误。(CVE-2017-3735)

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 192.168.31.187 | 8090 |

* 加固建议：

OpenSSL Project已经为此发布了一个安全公告（FreeBSD-SA-17:11.openssl）以及相应补丁: FreeBSD-SA-17:11.openssl：OpenSSL multiple vulnerabilities 链接：https://security.FreeBSD.org/advisories/FreeBSD-SA-17:11.openssl.asc

* + 1. 【中危】OpenSSL 1.0.2<1.0.2n多个漏洞
* 漏洞描述：

根据它的横幅，在远程主机上运行的OpenSSL版本是1.0。x在1.0.2n之前。因此，它受到多个漏洞的影响，这些漏洞可能会导致私钥信息恢复或数据无法正确加密。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 192.168.31.187 | 8090 |

* 加固建议：

升级至OpenSSL 1.0.2n或更高版本。

* + 1. 【中危】OpenSSL 资源管理错误漏洞
* 漏洞描述：

OpenSSL是OpenSSL团队的一个开源的能够实现安全套接层（SSLv2/v3）和安全传输层（TLSv1）协议的通用加密库。该产品支持多种加密算法，包括对称密码、哈希算法、安全散列算法等。 OpenSSL 1.1.0版本至1.1.0g版本和1.0.2b版本至1.0.2n版本中存在资源管理错误漏洞。该漏洞源于网络系统或产品对系统资源（如内存、磁盘空间、文件等）的管理不当。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 192.168.31.187 | 8090 |

* 加固建议：

厂商已发布升级补丁以修复漏洞，补丁获取链接： https://www.openssl.org/news/secadv/20180327.txt

* + 1. 【中危】OpenSSL 加密问题漏洞
* 漏洞描述：

OpenSSL 1.1.0版本至1.1.0h版本和1.0.2版本至1.0.2o版本中存在加密问题漏洞。该漏洞源于网络系统或产品未正确使用相关密码算法，导致内容未正确加密、弱加密、明文存储敏感信息等。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 192.168.31.187 | 8090 |

* 加固建议：

厂商已发布升级补丁以修复漏洞，补丁获取链接： https://www.openssl.org/news/secadv/20180612.txt

* + 1. 【中危】Apache HTTP Server 安全漏洞
* 漏洞描述：

Apache HTTP Server 2.4.17版本至2.4.34版本中存在安全漏洞。攻击者可通过持续发送较大的SETTINGS帧利用该漏洞在客户端占据连接，服务器线程和CPU时间时造成连接超时失效，导致拒绝服务。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 192.168.31.187 | 8090 |

* 加固建议：

目前厂商已发布升级补丁以修复漏洞，补丁获取链接： https://httpd.apache.org/security/vulnerabilities\_24.html

* + 1. 【中危】OpenSSL 信息泄露漏洞
* 漏洞描述：

OpenSSL是OpenSSL团队的一个开源的能够实现安全套接层（SSLv2/v3）和安全传输层（TLSv1）协议的通用加密库。该产品支持多种加密算法，包括对称密码、哈希算法、安全散列算法等。 OpenSSL中存在信息泄露漏洞。该漏洞源于网络系统或产品在运行过程中存在配置等错误。未授权的攻击者可利用漏洞获取受影响组件敏感信息。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 192.168.31.187 | 8090 |

* 加固建议：

厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法： https://github.com/bbbrumley/portsmash

* + 1. 【中危】OpenSSL 信息泄露漏洞
* 漏洞描述：

OpenSSL是OpenSSL团队的一个开源的能够实现安全套接层（SSLv2/v3）和安全传输层（TLSv1）协议的通用加密库。该产品支持多种加密算法，包括对称密码、哈希算法、安全散列算法等。 OpenSSL 1.0.2版本中存在信息泄露漏洞。攻击者可利用该漏洞绕过访问限制，获取敏感信息。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 192.168.31.187 | 8090 |

* 加固建议：

厂商已发布升级补丁以修复漏洞，补丁获取链接： https://www.openssl.org/news/secadv/20190226.txt

* + 1. 【中危】OpenSSL 1.0.2<1.0.2t多个漏洞
* 漏洞描述：

安装在远程主机上的测试产品版本早于测试版本。因此，它受到多个漏洞的影响：-通常在OpenSSL EC组中，总是存在一个共同因素，这用于抗侧通道的代码路径。但是，在某些情况下，可以使用显式参数（而不是使用命名曲线）构造组。在这些情况下，这类群体可能不存在辅因子。即使所有参数都与已知的命名曲线匹配，也可能发生这种情况。如果使用这种曲线，那么OpenSSL会退回到非侧通道抗代码路径，这可能会导致ECDSA签名操作期间的完整密钥恢复。为了容易受到攻击，攻击者必须能够在使用libcrypto的应用程序使用显式参数且不存在辅因子的情况下，对大量签名的创建进行计时。为避免疑问，libssl不易受攻击，因为从未使用显式参数。OpenSSL版本1.1.1、1.1.0和1.0.2受此问题影响。（CVE-2019-1547）-OpenSSL具有目录树的内部默认值，在目录树中可以找到配置文件以及用于TLS中验证的证书。该目录通常被称为OPENSSLDIR，可以通过--prefix/--OPENSSLDIR配置选项进行配置。对于OpenSSL版本1.1.0和1.1.1，mingw配置目标假定生成的程序和库安装在类似Unix的环境中，程序安装和OPENSSLDIR的默认前缀应为“/usr/local”。然而，mingw程序是Windows程序，因此，他们发现自己正在查看“C:/usr/local”的子目录，这可能是世界范围内可写的，这使不受信任的用户能够修改OpenSSL的默认配置、插入CA证书、修改（甚至替换）现有引擎模块，等等。对于OpenSSL 1.0.2，“/usr/local/ssl”被用作所有Unix和Windows目标（包括Visual C构建）上OPENSSLDIR的默认值。然而，1.0.2上针对不同Windows目标的一些构建说明鼓励您指定自己的--prefix。OpenSSL版本1.1.1、1.1.0和1.0.2受此问题影响。由于受影响部署的范围有限，这已被评估为低严重性，因此我们目前不创建新版本。（CVE-2019-1552）-在攻击者收到解密尝试成功或失败的自动通知的情况下，攻击者在发送大量要解密的消息后，可以恢复CMS/PKCS7传输的加密密钥或解密任何使用RSA公钥加密的RSA加密消息，使用Bleichenbacher填充oracle攻击。如果应用程序将证书与专用RSA密钥一起用于CMS\_decrypt或PKCS7\_decrypt函数，以选择要解密的正确收件人信息，则不会受到影响。（CVE-2019-1563）请注意，Nessus没有针对这些问题进行测试，而是只依赖于应用程序的自我报告版本号。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 192.168.31.187 | 8090 |

* 加固建议：

升级至OpenSSL 1.0.2t或更高版本。

* + 1. 【中危】OpenSSL 1.0.2<1.0.2u过程溢出漏洞
* 漏洞描述：

远程主机上安装的OpenSSL版本早于1.0.2u。因此，它受到1.0.2u建议中提到的漏洞的影响。-x64\_64 Montgomery平方过程中存在溢出错误，该过程用于512位模的幂运算。没有EC算法受到影响。分析表明，由于该缺陷，对2-prime RSA1024、3-prime RSA1536和DSA1024的攻击将非常难以执行，而且据信不太可能。针对DH512的攻击被认为是可行的。但是，对于攻击，目标必须重新使用DH512私钥，无论如何都不建议这样做。此外，如果直接使用低级API BN\_mod\_exp的应用程序使用BN\_FLG\_CONSTTIME，可能会受到影响。在OpenSSL 1.1.1e-dev中修复（受影响1.1.1-1.1.1d）。在OpenSSL 1.0.2u-dev中修复（受影响1.0.2-1.0.2t）。（CVE-2019-1551）请注意，Nessus没有针对该问题进行测试，而是仅依赖于应用程序的自我报告版本号。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 192.168.31.187 | 8090 |

* 加固建议：

升级至OpenSSL 1.0.2u或更高版本。

* + 1. 【中危】Apache 2.4.x < 2.4.42 多种漏洞
* 漏洞描述：

远程主机上安装的Apache httpd版本在2.4.42之前。因此，它受到2.4.42咨询中提到的多个漏洞的影响。-在Apache HTTP服务器2.4.0到2.4.41,mod\_proxy\_ftp可能使用未初始化的内存当代理到一个恶意的FTP服务器。在Apache HTTP Server 2.4.0到2.4.41中，用mod\_rewrite配置的意图是自引用的重定向可能会被编码的新行所欺骗，而重定向到请求URL中一个意外的URL。(CVE-2020-1927)请注意，Nessus没有对此问题进行测试，而是只依赖于应用程序自己报告的版本号。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 192.168.31.187 | 8090 |

* 加固建议：

升级到Apache 2.4.42或更高版本。

* + 1. 【中危】OpenSSL 1.0.2<1.0.2x空指针解引用漏洞
* 漏洞描述：

安装在远程主机上的测试产品版本早于测试版本。因此，它受到1.0.2x建议中提到的漏洞的影响。-X.509 GeneralName类型是一种泛型类型，用于表示不同类型的名称。其中一种名称类型称为EdPartyName。OpenSSL提供了一个函数GENERAL\_NAME\_cmp，它比较GENERAL\_NAME的不同实例，看看它们是否相等。当两个通用名称都包含EDIPARTYNAME时，此函数的行为不正确。可能会发生空指针解引用和崩溃，从而导致可能的拒绝服务攻击。OpenSSL本身使用GENERAL\_NAME\_cmp函数有两个目的：1）比较可用CRL和X509证书中嵌入的CRL分发点之间的CRL分发点名称2）验证时间戳响应令牌签名者是否与时间戳权限名称匹配（通过API函数TS\_RESP\_verify\_response和TS\_RESP\_verify\_token公开）如果攻击者可以控制正在比较的两个项目，则攻击者可能会触发崩溃。例如，如果攻击者可以诱使客户端或服务器根据恶意CRL检查恶意证书，则可能会发生这种情况。请注意，有些应用程序会根据证书中嵌入的URL自动下载CRL。该检查在验证证书和CRL上的签名之前进行。OpenSSL的\_服务器、s\_客户端和验证工具都支持-crl\_下载选项，该选项实现了自动crl下载，并且已证明该攻击可针对这些工具。请注意，一个不相关的错误意味着受影响的OpenSSL版本无法解析或构造正确的EDIPARTYNAME编码。然而，有可能构造一个格式错误的ePartyName，OpenSSL的解析器将接受它，从而触发此攻击。所有OpenSSL 1.1.1和1.0.2版本都受此问题影响。其他OpenSSL版本不受支持，尚未检查。在OpenSSL 1.1.1i中修复（受1.1.1-1.1.1h影响）。在OpenSSL 1.0.2x中修复（受影响1.0.2-1.0.2w）。（CVE-2020-1971）请注意，Nessus没有针对这个问题进行测试，而是只依赖于应用程序的自我报告版本号。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 192.168.31.187 | 8090 |

* 加固建议：

升级至OpenSSL 1.0.2x或更高版本。

* + 1. 【中危】PHP<7.3.28电子邮件头插入
* 漏洞描述：

根据其自我报告的版本号，在远程web服务器上运行的PHP版本早于7.3.28。因此，由于未能正确处理标头字段中的CR-LF序列，它会受到电子邮件标头注入漏洞的影响。未经验证的远程攻击者可以通过在电子邮件头中插入换行符来利用此漏洞，以获得对电子邮件头内容的完全控制。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 192.168.31.187 | 8090 |

* 加固建议：

升级至PHP 7.3.28或更高版本。

* + 1. 【中危】OpenSSL 1.0.2<1.0.2zc-dev漏洞
* 漏洞描述：

远程主机上安装的OpenSSL版本早于1.0.2zc-dev。因此，它受到1.0.2zx-dev建议中提到的漏洞的影响。-MIPS32和MIPS64平方过程中存在进位传播错误。许多EC算法都受到影响，包括一些TLS 1.3默认曲线。没有详细分析影响，因为攻击的先决条件被认为不太可能，包括重用私钥。分析表明，由于该缺陷而对RSA和DSA进行的攻击将非常难以执行，而且据信不太可能。对DH的攻击被认为是可行的（尽管非常困难），因为推断关于私钥的信息所需的大部分工作可以离线执行。这种攻击所需的资源量将是巨大的。然而，要使TLS攻击有意义，服务器必须在多个客户端之间共享DH私钥，这在CVE-2016-0701之后不再是一个选项。此问题影响OpenSSL 1.0.2、1.1.1和3.0.0版本。2021 12月15日发布的1.1.1万和3.01万版本中解决了这一问题。对于1.0.2版本，它是在gitcommit 6fc1aaf3中解决的，该版本仅适用于高级支持客户。它将在1.0.2zc中发布。该问题仅影响MIPS平台上的OpenSSL。在OpenSSL 3.0.1中修复（受影响的3.0.0）。在OpenSSL 1.1.1m中修复（受到影响的1.1.1-1.1l）。在OpenSSL 1.0.2zc-dev中修复了（受影响1.0.2-1.0.2zb）。（CVE-221-4160）请注意，Nessus尚未测试此问题，但只依赖于应用程序的自报告版本号。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 192.168.31.187 | 8090 |

* 加固建议：

升级至OpenSSL 1.0.2zc-dev或更高版本。

* + 1. 【低危】Web服务器传输明文凭证
* 漏洞描述：

远程web服务器包含几个HTML表单字段，其中包含“password”类型的输入，这些输入以明文形式将其信息传输到远程web服务器。窃听web浏览器和服务器之间通信的攻击者可能获得有效用户的登录名和密码。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 192.168.31.187 | 8090 |

* 加固建议：

确保每个敏感表单都通过HTTPS传输内容。

* + 1. 【低危】OpenSSL 1.0.2<1.0.2w信息披露
* 漏洞描述：

远程主机上安装的OpenSSL版本是1.0.2之前的1.0.2w。因此，它受到1.0.2w建议中提到的漏洞的影响。浣熊攻击利用TLS规范中的一个漏洞，该漏洞可能导致攻击者能够在使用基于Diffie Hellman（DH）的密码套件的连接中计算主密钥前的秘密。在这种情况下，这将导致攻击者能够窃听通过该TLS连接发送的所有加密通信。只有在实现跨多个TLS连接重新使用DH机密时，才能利用该攻击。请注意，此问题仅影响DH ciphersuites，而不影响ECDH ciphersuites。请注意，Nessus没有针对这个问题进行测试，而是只依赖于应用程序的自我报告版本号。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 192.168.31.187 | 8090 |

* 加固建议：

升级至OpenSSL版本1.0.2w或更高版本。

* + 1. 【低危】OpenSSL 1.0.2<1.0.2y多个漏洞
* 漏洞描述：

安装在远程主机上的测试产品版本早于测试版本。因此，它受到1.0.2y咨询中提到的多个漏洞的影响。-OpenSSL公共API函数X509\_issuer\_和\_serial\_hash（）尝试基于X509证书中包含的颁发者和序列号数据创建唯一的哈希值。但是，它无法正确处理解析issuer字段时可能发生的任何错误（如果issuer字段是恶意构造的，则可能会发生错误）。这可能会导致空指针失效和崩溃，从而导致潜在的拒绝服务攻击。OpenSSL本身从未直接调用函数X509\_issuer\_和\_serial\_hash（），因此只有当应用程序直接使用该函数，并在可能从不受信任的来源获取的证书上使用该函数时，应用程序才会受到攻击。OpenSSL版本1.1.1i及以下版本受此问题影响。这些版本的用户应该升级到OpenSSL 1.1.1j。OpenSSL 1.0.2x及以下版本受此问题影响。然而，OpenSSL 1.0.2已不受支持，不再接收公共更新。OpenSSL 1.0.2的高级支持客户应升级到1.0.2y。其他用户应升级至1.1.1j。在OpenSSL 1.1.1j中修复（受1.1.1-1.1.1i影响）。在OpenSSL 1.0.2y中修复（受影响1.0.2-1.0.2x）。（CVE-2021-23841）-在某些情况下，对EVP\_CipherUpdate、EVP\_EncryptUpdate和EVP\_DecryptUpdate的调用可能会使输出长度参数溢出，其中输入长度接近平台上整数的最大允许长度。在这种情况下，函数调用的返回值将为1（表示成功），但输出长度值将为负值。这可能会导致应用程序行为不正确或崩溃。OpenSSL版本1.1.1i及以下版本受此问题影响。这些版本的用户应该升级到OpenSSL 1.1.1j。OpenSSL 1.0.2x及以下版本受此问题影响。然而，OpenSSL 1.0.2已不受支持，不再接收公共更新。OpenSSL 1.0.2的高级支持客户应升级到1.0.2y。其他用户应升级至1.1.1j。在OpenSSL 1.1.1j中修复（受1.1.1-1.1.1i影响）。在OpenSSL 1.0.2y中修复（受影响1.0.2-1.0.2x）。（CVE-2021-23840）-OpenSSL 1.0.2支持SSLv2。如果客户机试图与配置为同时支持SSLv2和更新的SSL和TLS版本的服务器协商SSLv2，则在添加RSA签名时会检查版本回滚攻击。支持SSL或TLS版本大于SSLv2的客户端应该使用特殊形式的填充。支持大于SSLv2的服务器应该拒绝来自存在这种特殊填充形式的客户端的连接尝试，因为这表明发生了版本回滚（即客户端和服务器都支持大于SSLv2的版本，但这是被请求的版本）。这种填充检查的实现颠倒了逻辑，因此，如果存在填充，连接尝试将被接受，如果不存在填充，连接尝试将被拒绝。这意味着，如果发生版本回滚攻击，例如服务器将接受连接。此外，如果尝试正常的SSLv2连接，服务器将错误地拒绝连接。只有版本1.0.2s到1.0.2x的OpenSSL 1.0.2服务器受此问题影响。为了使1.0.2服务器易受攻击，必须：1）在编译时配置了SSLv2支持（默认为关闭），2）在运行时配置了SSLv2支持（默认为关闭），3）已配置SSLv2密码套件（这些不在默认密码套件列表中）OpenSSL 1.1.1不支持SSLv2，因此不易受到此问题的攻击。基本错误是在RSA\_padding\_check\_SSLv23（）函数的实现中。这也会影响其他各种函数使用的RSA\_SSLV23\_填充模式。尽管1.1.1不支持SSLv2，但RSA\_padding\_check\_SSLv23（）函数仍然存在，RSA\_SSLv23\_padding模式也是如此。直接调用该函数或使用该填充模式的应用程序将遇到此问题。但是，由于1.1.1中不支持SSLv2协议，因此在该版本中，这被视为一个错误，而不是安全问题。OpenSSL 1.0.2已不受支持，不再接收公共更新。OpenSSL 1.0.2的高级支持客户应升级到1.0.2y。其他用户应升级至1.1.1j。在OpenSSL 1.0.2y中修复（受影响1.0.2s-1.0.2x）。（CVE-2021-23839）请注意，Nessus没有针对这个问题进行测试，而是只依赖于应用程序的自我报告版本号。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 192.168.31.187 | 8090 |

* 加固建议：

升级至OpenSSL版本1.0.2y或更高版本。