|  |  |  |
| --- | --- | --- |
| **Oracle** **数据库和中间件产品的安全漏洞常见问题** **(Doc ID 2301393.1)** | [IMG_256](https://support.oracle.com/epmos/faces/DocumentDisplay?_afrLoop=329461985410286%26id=2301393.1%26_adf.ctrl-state=z5jm6lzen_167%20/o%20To%20Bottom)  [To Bottom](https://support.oracle.com/epmos/faces/DocumentDisplay?_afrLoop=329461985410286&id=2301393.1&_adf.ctrl-state=z5jm6lzen_167 \\o To Bottom) | IMG_257 |

IMG_258

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **文档内容**   |  |  | | --- | --- | |  | [用途](https://support.oracle.com/epmos/faces/DocumentDisplay?_afrLoop=329461985410286&id=2301393.1&_adf.ctrl-state=z5jm6lzen_167 \\l PURPOSE) |  |  |  | | --- | --- | |  | [Oracle 安全警报和漏洞修复策略/过程](https://support.oracle.com/epmos/faces/DocumentDisplay?_afrLoop=329461985410286&id=2301393.1&_adf.ctrl-state=z5jm6lzen_167 \\l aref_section11) |  |  |  | | --- | --- | |  | [热门请求:](https://support.oracle.com/epmos/faces/DocumentDisplay?_afrLoop=329461985410286&id=2301393.1&_adf.ctrl-state=z5jm6lzen_167 \\l aref_section12) |  |  |  | | --- | --- | |  | [CVE-2015-4852 - Deserialization Vulnerability](https://support.oracle.com/epmos/faces/DocumentDisplay?_afrLoop=329461985410286&id=2301393.1&_adf.ctrl-state=z5jm6lzen_167 \\l aref_section13) |  |  |  | | --- | --- | |  | [CVE-2014-3566 - SSL V3.0 "Poodle" Vulnerability](https://support.oracle.com/epmos/faces/DocumentDisplay?_afrLoop=329461985410286&id=2301393.1&_adf.ctrl-state=z5jm6lzen_167 \\l aref_section14) |  |  |  | | --- | --- | |  | [CVE-2014-0160 - OpenSSL Security Bug - Heartbleed](https://support.oracle.com/epmos/faces/DocumentDisplay?_afrLoop=329461985410286&id=2301393.1&_adf.ctrl-state=z5jm6lzen_167 \\l aref_section15) |  |  |  | | --- | --- | |  | [问题和答案](https://support.oracle.com/epmos/faces/DocumentDisplay?_afrLoop=329461985410286&id=2301393.1&_adf.ctrl-state=z5jm6lzen_167 \\l FAQ) |  |  |  | | --- | --- | |  | [PART I: 所有Oracle产品的常见漏洞](https://support.oracle.com/epmos/faces/DocumentDisplay?_afrLoop=329461985410286&id=2301393.1&_adf.ctrl-state=z5jm6lzen_167 \\l aref_section21) |  |  |  | | --- | --- | |  | [1.第一步](https://support.oracle.com/epmos/faces/DocumentDisplay?_afrLoop=329461985410286&id=2301393.1&_adf.ctrl-state=z5jm6lzen_167 \\l aref_section22) |  |  |  | | --- | --- | |  | [2. 漏洞信息](https://support.oracle.com/epmos/faces/DocumentDisplay?_afrLoop=329461985410286&id=2301393.1&_adf.ctrl-state=z5jm6lzen_167 \\l aref_section23) |  |  |  | | --- | --- | |  | [3. 扫描报告](https://support.oracle.com/epmos/faces/DocumentDisplay?_afrLoop=329461985410286&id=2301393.1&_adf.ctrl-state=z5jm6lzen_167 \\l aref_section24) |  |  |  | | --- | --- | |  | [4. 研究某个CVE](https://support.oracle.com/epmos/faces/DocumentDisplay?_afrLoop=329461985410286&id=2301393.1&_adf.ctrl-state=z5jm6lzen_167 \\l aref_section25) |  |  |  | | --- | --- | |  | [5. 怎样新开一个关于安全漏洞的Service Request](https://support.oracle.com/epmos/faces/DocumentDisplay?_afrLoop=329461985410286&id=2301393.1&_adf.ctrl-state=z5jm6lzen_167 \\l aref_section26) |  |  |  | | --- | --- | |  | [PART II: WebLogic Serverc安全漏洞FAQ](https://support.oracle.com/epmos/faces/DocumentDisplay?_afrLoop=329461985410286&id=2301393.1&_adf.ctrl-state=z5jm6lzen_167 \\l aref_section27) |  |  |  | | --- | --- | |  | [1. 第一步](https://support.oracle.com/epmos/faces/DocumentDisplay?_afrLoop=329461985410286&id=2301393.1&_adf.ctrl-state=z5jm6lzen_167 \\l aref_section28) |  |  |  | | --- | --- | |  | [2. 安全最佳实践](https://support.oracle.com/epmos/faces/DocumentDisplay?_afrLoop=329461985410286&id=2301393.1&_adf.ctrl-state=z5jm6lzen_167 \\l aref_section29) |  |  |  | | --- | --- | |  | [PART III: Oracle Fusion Middleware (10g/11g/12c)安全漏洞FAQ](https://support.oracle.com/epmos/faces/DocumentDisplay?_afrLoop=329461985410286&id=2301393.1&_adf.ctrl-state=z5jm6lzen_167 \\l aref_section210) |  |  |  | | --- | --- | |  | [1. 第一步](https://support.oracle.com/epmos/faces/DocumentDisplay?_afrLoop=329461985410286&id=2301393.1&_adf.ctrl-state=z5jm6lzen_167 \\l aref_section211) |  |  |  | | --- | --- | |  | [2. 安全最佳实践](https://support.oracle.com/epmos/faces/DocumentDisplay?_afrLoop=329461985410286&id=2301393.1&_adf.ctrl-state=z5jm6lzen_167 \\l aref_section212) |  |  |  | | --- | --- | |  | [3. Apache 的安全漏洞](https://support.oracle.com/epmos/faces/DocumentDisplay?_afrLoop=329461985410286&id=2301393.1&_adf.ctrl-state=z5jm6lzen_167 \\l aref_section213) |  |  |  | | --- | --- | |  | [4. Java 的安全漏洞](https://support.oracle.com/epmos/faces/DocumentDisplay?_afrLoop=329461985410286&id=2301393.1&_adf.ctrl-state=z5jm6lzen_167 \\l aref_section214) |  |  |  | | --- | --- | |  | [参考](https://support.oracle.com/epmos/faces/DocumentDisplay?_afrLoop=329461985410286&id=2301393.1&_adf.ctrl-state=z5jm6lzen_167 \\l REF) |     **适用于:**  Oracle WebLogic Server - 版本 9.0 和更高版本  Oracle Fusion Middleware - 版本 10.1.2.0.0 和更高版本  Oracle Database - Enterprise Edition - 版本 10.1.0.5 和更高版本  本文档所含信息适用于所有平台  **用途**  **Oracle** **安全警报和漏洞修复策略/过程**  这篇文档提供了如何处理Oracle产品中可疑的漏洞相关信息。在此FAQ中提供的问题和答案都来源于以下Oracle安全网站：  重要补丁更新和安全警报  [https://www.oracle.com/technetwork/topics/security/alerts-086861.html](https://www.oracle.com/technetwork/topics/security/alerts-086861.html /t _blank)  安全漏洞修复政策和流程  **热门请求:**  **CVE-2015-4852 - Deserialization Vulnerability**  <https://www.oracle.com/technetwork/topics/security/alert-cve-2015-4852-2763333.html>  [Note 2075927.1](https://support.oracle.com/epmos/faces/DocumentDisplay?parent=DOCUMENT&sourceId=2301393.1&id=2075927.1) CVE-2015-4852 Patch Availability Document for Oracle WebLogic Server Component of Oracle Fusion Middleware  [Note 2076338.1](https://support.oracle.com/epmos/faces/DocumentDisplay?parent=DOCUMENT&sourceId=2301393.1&id=2076338.1) CVE-2015-4852 Mitigation Recommendations for Oracle WebLogic Server Component of Oracle Fusion Middleware  **CVE-2014-3566 - SSL V3.0 "Poodle" Vulnerability**  <https://www.oracle.com/technetwork/topics/security/poodlecve-2014-3566-2339408.html>  [Note 1936300.1](https://support.oracle.com/epmos/faces/DocumentDisplay?parent=DOCUMENT&sourceId=2301393.1&id=1936300.1) How to Change SSL Protocols (to Disable SSL 2.0/3.0) in Oracle WebLogic Server & Fusion Middleware Products  **CVE-2014-0160 - OpenSSL Security Bug - Heartbleed**  <https://www.oracle.com/technetwork/topics/security/alert-cve-2014-0160-2190703.html>  and  <https://www.oracle.com/technetwork/topics/security/opensslheartbleedcve-2014-0160-2188454.html>  *重要:* *这不是完整列表*, 请参考上面的重要补丁更新和安全警报页面*.*  **问题和答案**  **PART I:** **所有Oracle产品的常见漏洞**  **1.第一步**  想保护我的Oracle产品不受已知的安全漏洞影响，首先该采取什么行动？  **回答:**  应用最新的补丁集，然后再应用重要补丁更新（CPU）。Oracle每季度都会发布最新的重要补丁更新（CPU）：每年的一月，四月，七月和10月。你应该保持更新来保护您的系统。请注意，所有补丁集是累积的，都会加到下一补丁集，所有还在错误修复日期内的版本都有相应的CPU。为了获得CPU，Oracle建议从查看以下链接内容开始：  **重要补丁更新（CPU）和安全警报**  <http://www.oracle.com/technetwork/topics/security/alerts-086861.html>  • 为了获取补丁，检查最新的安全通告和补丁可用性文档  • 安全顾问文档记录着特定的CPU版本修复的漏洞。  • 补丁可用性文档提供了在受支持的版本的累积补丁(Note 209768.1)  **2.** **漏洞信息**  我在互联网上发现潜在的漏洞，现在想知道它对Oracle产品的影响。我可以从哪里获得Oracle关于此漏洞的信息？  **回答**：  Oracle不会对外界所说的安全漏洞对Oracle产品的影响作出任何评价。当Oracle得知有这样的漏洞，Oracle将作出全面调查。如有必要，在下一个版本，安全警报和/或季度重要补丁更新里作出修复。  请注意，在许多情况下，网上说的脆弱性的报告不太准确，因为：  • 影响是不准确的  • 访问或版本信息不准确  • 可能没有bug，或者它可能不是一个安全漏洞  • 拟议的解决方法可能对某些环境上无效的。  • 拟议的解决方法可能会导致其他问题。  Oracle建议客户从重要补丁更新公告获取所有的安全漏洞信息，链接如下：  <http://www.oracle.com/technetwork/topics/security/alerts-086861.html>  Oracle感谢那些向Oracle报告漏洞的个人，因为这有助于Oracle为所有的客户提升其产品质量。  解释  关于外部描述的漏洞有些人会问很多问题。在很多情况下，我们的答案会基于一个原则，即“Oracle不会泄露，有可能有助于攻击者会用来攻击Oracle产品的信息”。当然，还有其他方面的考虑：  • 很多时候我们不能完全确定外面爆出来的一些漏洞，所以当然也不能对它做评论。  • 很多时候我们知道报道是不准确的。如果我们通知这些信息不准确的网站，该网站会让我们提供准确的信息，但这些信息将有助于黑客攻击的切入点。  • 变通方法很少会试用于所有环境。如果去解释什么场景下变通办法有效或无效，会给黑客提供关键信息。  • 如果我们提供特定CPU都修复了哪些漏洞信息，黑客能得出尚未修复的漏洞是哪些。这可以让他们集中他们的攻击显著帮助攻击者。  • 一般政策是，Oracle不会对是否或何时修复外部报告的漏洞等问题做解释。  **3.** **扫描报告**  我使用第三方安全扫描工具检测到一个潜在漏洞而且已经应用了最新的重要补丁更新，但是扫描结果都是一样的。供应商建议做一些配置解决这个问题。关于这个扫描报告，我在Oracle哪里能得到相关信息？  答案：  我们不知道第三方安全扫描有没有真正扫描到暴露的安全漏洞，或是检查一下版本什么的，然后显示出该版本有可能存在的漏洞。这需要跟扫描服务商联系，确认它是否考虑到Oracle产品上应用了的CPU。供应商也可以联系Oracle安全部门协作来报告安全漏洞，和/或检查特定的CPU有没有解决特定漏洞。  报告安全漏洞  [https://www.oracle.com/technetwork/topics/security/alerts-086861.html#ReportingVulnerabilities](https://www.oracle.com/technetwork/topics/security/alerts-086861.html /l ReportingVulnerabilities)  安全漏洞修复政策和流程  [https://www.oracle.com/support/assurance/vulnerability-remediation/security-fixing.html](https://www.oracle.com/support/assurance/vulnerability-remediation/security-fixing.html /t _blank)    如果需要在My Oracle Support上创建服务请求（SR），应明确描述，并问题提供足够的信息来再现可能的漏洞。 Oracle技术支持无法对第三方扫描报告进行解释。详细请参见创建SR的常见问题。  注意，这些政策同样适用于惩罚性测试组织。  为了防止任何已知的，已修复的漏洞，请应用最新的重要补丁更新(CPU)。如果你有一个新的漏洞，请提供一个可以复现问题的Test Case给Oracle。Oracle会审查已经提交在[http://cve.mitre.org](http://cve.mitre.org/)和[http://nvd.nist.gov](http://nvd.nist.gov/)上的可能会影响Oracle产品的所有公共漏洞。  [Note 2131521.1](https://support.oracle.com/epmos/faces/DocumentDisplay?parent=DOCUMENT&sourceId=2301393.1&id=2131521.1) Proactively Updating SSL Protocols, Ciphers, and Certificates for Oracle Fusion Middleware  **4.** **研究某个CVE**  我需要询问Oracle关于一个Common Vulnerabilities and Exposures (CVE).我理解Oracle不会对此提供评价，但是我怎样研究这样的问题?  **回答:**  Common Vulnerabilities and Exposures (CVE) 用于跟踪安全漏洞。<http://cve.mitre.org/>提供CVE编号和其它信息。Oracle Security 查看这些CVE是否需要在Oracle产品上修复。要调查一个CVE，你可以从查看 [https://cve.mitre.org/](http://cve.mitre.org/) 开始. 也可参考NVD 网站 ([https://nvd.nist.gov/](http://nvd.nist.gov/ /t _blank)). 如果是第三方的安全顾问提供的，请先询问是否有已知的安全建议提供给你.  **Step 1:** 查看CVE号码:  <https://cve.mitre.org/cgi-bin/cvename.cgi?name=>  **Step 2:** 在Oracle 网站上查看Oracle产品修复的CVE:  Map of Public Vulnerability to Advisory/Alert  <https://www.oracle.com/technetwork/topics/security/public-vuln-to-advisory-mapping-093627.html>  **Step 3:** 如果您在上述列表中找到CVE，请单击“咨询”链接。如果CVE有多次发生，可能是针对不同的产品。检查咨询并搜索CVE的页面，看看它是否适用于您的产品。如果是这样，请检查行中提供的所有信息，包括脚注。  **Step 4:** 要查看CVE的基于文本的摘要，请在同一个咨询页面上，转到“References”部分，然后单击“English text version of the risk matrices”链接。然后可以使用方便的复制/粘贴版本供您使用。  **Step 5:** 顾问文档页面” Risk Matrices”部分会列出这个CVE编号以及影响的Oracle产品和版本。还有链接到CPU补丁可用性文档(Critical Patch Update Patch Availability Documents),你可以在这个文档（Patch Availability Documents）搜索这个CVE编号，文档会列出CVE(s)和修复它的Patch。CVE只出现在它第一次被修复的CPU补丁可用性文档中。新的CPU补丁可用性文档（Patch Availability Documents）不列出过去的CVE编号。   * 如果你发现新的漏洞利用请立即报告给Oracle。 * 不管你的第三方安全扫描报告的CVE是否出现在上述列表，你都需要在报告时提供漏洞利用的详细重现步骤。如果第三方顾问建议你追查,Oracle 技术支持可以根据Oracle技术支持策略帮助你。 * 如果CVE没有被列举在任何上述文档，Oracle技术支持也就不能提供关于这个CVE的任何信息。这个流程遵循下面的文档：   Security Vulnerability Fixing Policy and Process  [https://www.oracle.com/support/assurance/vulnerability-remediation/security-fixing.html](https://www.oracle.com/support/assurance/vulnerability-remediation/security-fixing.html /t _blank)    **5.** **怎样新开一个关于安全漏洞的Service Request**  我要报告一个可疑的安全漏洞，我应该怎样新开一个Service Request (SR)给Oracle技术支持，我能希望获得什么样的帮助?  **回答:**  Oracle 技术支持工程师会帮助客户向Oracle安全部门报告新的安全漏洞, 提供已知安全漏洞的文档位置,或者帮助客户配置最佳实践.为了保护所有客户，Oracle的策略是不评价和透露任何特定潜在的和确实存在的安全漏洞。这个FAQ文档回答了常见问题，如果有其它特定情况，下面列出了准备事项和新开SR步骤:   * 查看这个FAQ文档。并确认最新的CPU已经安装 * 准备上传 CPU patch 的 log 文件确认没有隐藏的错误或者错过的组件。 * 如果有第三方的建议和扫描报告，请确保清楚说明要从Oracle获得哪些组件的哪些帮助。 * 如果要报告一个新的漏洞，请提供详细重现步骤或者扫描报告。       **PART II: WebLogic Serverc安全漏洞FAQ**  **1.** **第一步**  以下关于安全漏洞和安全策略的适用于所有Oracle WebLogic Server 版本。  查看安全通报时，请参阅标记为“Oracle Fusion Middleware”的“修补程序可用性文档”链接（这是许多产品共享的相同文档）。达到此文档时，如果您在FMW 11g环境中安装并使用Oracle WebLogic，请查看“Oracle融合中间件11g”部分。如果单独使用Oracle WebLogic Server或10.3.1版本，请检查“Oracle Weblogic Server”部分。  Oracle 建议从下面的链接开始获得最新的安全建议:  Critical Patch Updates (CPU) and Security Alerts  <http://www.oracle.com/technetwork/topics/security/alerts-086861.html>   * 检查最新的安全顾问文档和修补程序可用性文档 * 每个CPU发布都有自己的一个修补程序可用性文档 * 修补程序可用性文档提供了在错误修复期内的产品的累计的补丁信息。 关于错误修复期请查看 [Note 950131.1](https://support.oracle.com/epmos/faces/DocumentDisplay?parent=DOCUMENT&sourceId=2301393.1&id=950131.1) , "*Error Correction Support Dates for Oracle WebLogic Server*" * 文档内的"Oracle Fusion Middleware" and/or "Oracle WebLogic Server" 部分说明了安全补丁和对应的包含这些安全补丁的Patch Set Updates (PSUs)     **2.** **安全最佳实践**  我已经安装了最新的Patch Set Update (PSU) ，还有其它的WebLogic Server安全配置的最佳实践吗？  **回答:**  Oracle 网站已经包含这样的最佳实践.取决于您的使用方式,WebLogic Server的组件提供各种安全配置选项。产品文档中有管理和安全指南部分可以参考。还建议聘请一名可以研究您的业务需求并提供建议的安全顾问。参考以下链接:  Oracle Fusion Middleware Securing Oracle WebLogic Server 11g Release 1 (10.3.6)  [http://docs.oracle.com/cd/E23943\_01/web.1111/e13707/toc.htm](http://docs.oracle.com/cd/E23943_01/web.1111/e13707/toc.htm /t _blank)  12 Configuring SSL  [http://docs.oracle.com/cd/E23943\_01/web.1111/e13707/ssl.htm#i1200848](http://docs.oracle.com/cd/E23943_01/web.1111/e13707/ssl.htm" \l "i1200848)  Add the <cookie-secure>true</cookie-secure> tag inside the <session-descriptor> element to the weblogic.xml file:  [http://docs.oracle.com/cd/E28280\_01/web.1111/e13712/weblogic\_xml.htm#r15c1-t9](http://docs.oracle.com/cd/E28280_01/web.1111/e13712/weblogic_xml.htm /l r15c1-t9 /t _blank)  Using Secure Cookies to Prevent Session Stealing  [http://docs.oracle.com/cd/E12840\_01/wls/docs103/security/thin\_client.html#wp1053780](http://docs.oracle.com/cd/E12840_01/wls/docs103/security/thin_client.html /l wp1053780 /t _blank)  Configure FRAME\_BUSTING context parameter to prevent clickjacking:  [https://docs.oracle.com/middleware/11119/adf/develop-faces/ap\_config.htm#BABDHGEJ](https://docs.oracle.com/middleware/11119/adf/develop-faces/ap_config.htm /l BABDHGEJ /t _blank)    Note 2131521.1 Proactively Updating SSL Protocols, Ciphers, and Certificates for Oracle Fusion Middleware  [Note 1936300.1](https://support.oracle.com/epmos/faces/DocumentDisplay?parent=DOCUMENT&sourceId=2301393.1&id=1936300.1) How to Change SSL Protocols (to Disable SSL 3.0) in Oracle Fusion Middleware Products  [Note 1067411.1](https://support.oracle.com/epmos/faces/DocumentDisplay?parent=DOCUMENT&sourceId=2301393.1&id=1067411.1) How To Disable Anonymous and Weak Cipher Suites In WebLogic Server  [Note 2040420.1](https://support.oracle.com/epmos/faces/DocumentDisplay?parent=DOCUMENT&sourceId=2301393.1&id=2040420.1) How to Configure the X-Frame-Options Header to Mitigate Clickjacking Attempts Using OHS and WLS Applications  [Note 1076314.1](https://support.oracle.com/epmos/faces/DocumentDisplay?parent=DOCUMENT&sourceId=2301393.1&id=1076314.1) How To Disable the HTTP methods other than GET and POST (such as PUT, DELETE, etc.) on a WebLogic Server Domain  [Note 2160221.1](https://support.oracle.com/epmos/faces/DocumentDisplay?parent=DOCUMENT&sourceId=2301393.1&id=2160221.1) How to Set HTTPOnly for a Secure HTTP Session Cookie in Various Fusion Middleware Applications  [Note 2075927.1](https://support.oracle.com/epmos/faces/DocumentDisplay?parent=DOCUMENT&sourceId=2301393.1&id=2075927.1) CVE-2015-4852 Patch Availability Document for Oracle WebLogic Server Component of Oracle Fusion Middleware  [Note 2076338.1](https://support.oracle.com/epmos/faces/DocumentDisplay?parent=DOCUMENT&sourceId=2301393.1&id=2076338.1) CVE-2015-4852 Mitigation Recommendations for Oracle WebLogic Server Component of Oracle Fusion Middleware  *Important: This is* ***not*** *a comprehensive list*    **PART III: Oracle Fusion Middleware (10g/11g/12c)安全漏洞FAQ**  **1.** **第一步**  本文的所有漏洞和安全策略信息适用于所有 Oracle Application Server (Oracle Fusion Middlware) 产品版本. 查看安全通报时，请参阅标记为“Oracle Fusion Middleware”的“修补程序可用性文档”链接（这是许多产品共享的相同文档）。到达此文档时，请查看Oracle Fusion Middleware 11g”部分。  Oracle 建议从下面的链接开始获得最新的安全建议:  Critical Patch Updates (CPU) and Security Alerts  <http://www.oracle.com/technetwork/topics/security/alerts-086861.html>   * 检查最新的安全顾问文档和修补程序可用性文档 * 每个CPU发布都有自己的一个修补程序可用性文档 * 修补程序可用性文档提供了在错误修复期内的产品的累计的补丁信息。 关于错误修复期请查看 Note 944866.1 - "*Error Correction Support Timelines for Oracle Application Server (Fusion Middleware)*"     **2.** **安全最佳实践**  我已经安装了最新的Patch Set Update (PSU) ，还有其它的安全配置的最佳实践吗？  **回答:**  根据您的使用情况，可能会为不同的安全性相关选项配置Oracle Fusion Middleware 产品的不同组件。这些将位于文档库中，其中有您正在管理的Oracle产品的管理和安全指南。还建议聘请一名可以研究您的业务需求并提供建议的安全顾问。比较流行的和安全最佳实践有关的技术支持文档列表:  [Note 2131521.1](https://support.oracle.com/epmos/faces/DocumentDisplay?parent=DOCUMENT&sourceId=2301393.1&id=2131521.1) Proactively Updating SSL Protocols, Ciphers, and Certificates for Oracle Fusion Middleware  [Note 2040420.1](https://support.oracle.com/epmos/faces/DocumentDisplay?parent=DOCUMENT&sourceId=2301393.1&id=2040420.1) How to Configure the X-Frame-Options Header to Mitigate Clickjacking Attempts Using OHS and WLS Applications  [Note 2160221.1](https://support.oracle.com/epmos/faces/DocumentDisplay?parent=DOCUMENT&sourceId=2301393.1&id=2160221.1) How to Set Secure and HTTPOnly Attributes on Cookies Sent from Various Oracle Fusion Middleware Applications  [Note 1936300.1](https://support.oracle.com/epmos/faces/DocumentDisplay?parent=DOCUMENT&sourceId=2301393.1&id=1936300.1) How to Change SSL Protocols (to Disable SSL 3.0) in Oracle Fusion Middleware Products  [Note 453079.1](https://support.oracle.com/epmos/faces/DocumentDisplay?parent=DOCUMENT&sourceId=2301393.1&id=453079.1) Restricting Anonymous or Weak Ciphers in SSL (HTTPS) for Oracle Fusion Middleware 10g/11g/12c  [Note 1905314.1](https://support.oracle.com/epmos/faces/DocumentDisplay?parent=DOCUMENT&sourceId=2301393.1&id=1905314.1) New SSL Protocol and Cipher Options for Oracle Fusion Middleware 11g OPMN/ONS  [Note 1677491.1](https://support.oracle.com/epmos/faces/DocumentDisplay?parent=DOCUMENT&sourceId=2301393.1&id=1677491.1) How to Configure Secure Cookies for EM Fusion Middleware Control 11g  [Note 1485047.1](https://support.oracle.com/epmos/faces/DocumentDisplay?parent=DOCUMENT&sourceId=2301393.1&id=1485047.1) Is SSLHonorCipherOrder and TLS 1.1/1.2 Supported for Oracle HTTP Server?  [Note 396604.1](https://support.oracle.com/epmos/faces/DocumentDisplay?parent=DOCUMENT&sourceId=2301393.1&id=396604.1) Controlling the Server Header with Oracle HTTP Server and Oracle Web Cache 10g/11g/12c  [Note 1915141.1](https://support.oracle.com/epmos/faces/DocumentDisplay?parent=DOCUMENT&sourceId=2301393.1&id=1915141.1) How To Disable ETag Header in Oracle HTTP Server  [Note 2026771.1](https://support.oracle.com/epmos/faces/DocumentDisplay?parent=DOCUMENT&sourceId=2301393.1&id=2026771.1) Is TLS\_FALLBACK\_SCSV Supported With Oracle HTTP Server?  Note 259404.1 How to Disable HTTP TRACE or Other REQUEST\_METHOD  [Note 1969719.1](https://support.oracle.com/epmos/faces/DocumentDisplay?parent=DOCUMENT&sourceId=2301393.1&id=1969719.1) How to Disable the Http TRACE REQUEST\_METHOD OC4J Standalone install  [Note 811605.1](https://support.oracle.com/epmos/faces/DocumentDisplay?parent=DOCUMENT&sourceId=2301393.1&id=811605.1) How To Disable WebDAV On HTTP Server or Portal  [Note 1301699.1](https://support.oracle.com/epmos/faces/DocumentDisplay?parent=DOCUMENT&sourceId=2301393.1&id=1301699.1) How the SSL/TLS Renegotiation Protocol Change Affects Oracle HTTP Server  Note 1218695.1 Master Note for SSL Configuration in Fusion Middleware 11g  [Note 341904.1](https://support.oracle.com/epmos/faces/DocumentDisplay?parent=DOCUMENT&sourceId=2301393.1&id=341904.1) Configuring HTTP Server to use SSL in Oracle Application Server 10g (10.1.2 - 10.1.3)  [Note 342155.1](https://support.oracle.com/epmos/faces/DocumentDisplay?parent=DOCUMENT&sourceId=2301393.1&id=342155.1) Configuring Web Cache with SSL in Oracle Application Server 10g Release 2 (10.1.2)  [Note 429286.1](https://support.oracle.com/epmos/faces/DocumentDisplay?parent=DOCUMENT&sourceId=2301393.1&id=429286.1) Configuring SSL Client Authentication with HTTP Server in Oracle Application Server 10g (10.1.2 - 10.1.3)  [Note 473029.1](https://support.oracle.com/epmos/faces/DocumentDisplay?parent=DOCUMENT&sourceId=2301393.1&id=473029.1) FIPS 140-2 Configuration with Oracle Application Server and HTTP Server 10g - doc link included for 11g  [Note 280165.1](https://support.oracle.com/epmos/faces/DocumentDisplay?parent=DOCUMENT&sourceId=2301393.1&id=280165.1) Troubleshooting Oracle HTTP Server Using /server-status (mod\_status)  [Note 311536.1](https://support.oracle.com/epmos/faces/DocumentDisplay?parent=DOCUMENT&sourceId=2301393.1&id=311536.1) Forbidden to Execute a PL/SQL Procedure With Parentheses  [Note 259576.1](https://support.oracle.com/epmos/faces/DocumentDisplay?parent=DOCUMENT&sourceId=2301393.1&id=259576.1) How to Redirect All Non-SSL Traffic On A Particular Port To SSL  [Note 827412.1](https://support.oracle.com/epmos/faces/DocumentDisplay?parent=DOCUMENT&sourceId=2301393.1&id=827412.1) How to Force >128bit Encryption with Oracle HTTP Server  **Oracle Reports**  - In 11.1.1.7, 11.1.2.1 and 11.1.2.2 CPU Docs:  [Note 1608683.1](https://support.oracle.com/epmos/faces/DocumentDisplay?parent=DOCUMENT&sourceId=2301393.1&id=1608683.1) Enable File System Access Control" - Fine Grained File System Access Control for the Reports Server  - In 11.1.1.4, 11.1.1.6, and 11.1.2.0 CPU Docs:  [Note 1479064.1](https://support.oracle.com/epmos/faces/DocumentDisplay?parent=DOCUMENT&sourceId=2301393.1&id=1479064.1) New Feature: <urlEngineAccess> Controls URLEngine (rwUrlEng) Sources:  [Note 1480206.1](https://support.oracle.com/epmos/faces/DocumentDisplay?parent=DOCUMENT&sourceId=2301393.1&id=1480206.1) REP-52262: Diagnostic Output is Disabled  - 10g (and as applicable to 11g in lieu of the above):  [Note 260243.1](https://support.oracle.com/epmos/faces/DocumentDisplay?parent=DOCUMENT&sourceId=2301393.1&id=260243.1) Using DIAGNOSTIC=NO (in rwservlet.properties) For Hiding Web Commands Like showmap, showenv, showjobs  [Note 234993.1](https://support.oracle.com/epmos/faces/DocumentDisplay?parent=DOCUMENT&sourceId=2301393.1&id=234993.1) Overview of the Reports URLEngine (rwURLEng)  *Important: This is* ***not*** *a comprehensive list*  **3. Apache** **的安全漏洞**  我们在使用 Oracle HTTP Server (OHS)，Apache Web Server的脆弱性报告说我们应该升级到更新的版本，应该怎么做呢？  **回答:**  Oracle Fusion Middleware产品安装的Oracle HTTP Server不能用Apache替代。OHS和Apache Web Server的打补丁和升级是不同的。Apache 组织可能用一个新版本修复问题和其它功能。Oracle 解决问题还要维护产品系列的兼容性。当Oracle开发或发布新版本时才会把新版本的 Apache 编译进来。  基于Apache 2.0的Oracle HTTP Server可以单独安装，并与原始配置结合使用，主要作为反向代理服务使用。在Oracle应用服务器10g框架下，不支持将已安装的基于Apache 1.3的Oracle HTTP Server升级到基于Apache 2.0的Oracle HTTP Server。使用Oracle Fusion Middleware 11g，可以使用基于Apache 2.2的Oracle HTTP Server。  如果安全漏洞报告来自Apache 安全警报,那么很可能会影响到OHS。Oracle的安全警报会对此进行确认,并提供相应的补丁。补丁会通过使用OHS的产品发布，以维护兼容性。基于Apache的版本可能保持不变，但该漏洞将被修复。 有些第三方的安全检测工具只会检查版本而不是检测漏洞本身，请咨询第三方工具提供商如何检测OHS.  总之，Oracle不会直接解决Apache 的安全漏洞问题. 需要在OHS上重现漏洞的利用。漏洞利用需要在OHS下重现。保持更新Oracle Fusion Middleware 补丁集以更新OHS,并安装最新的CPU，这是最好的保护系统的措施。  Reference:  [Note 260449.1](https://support.oracle.com/epmos/faces/DocumentDisplay?parent=DOCUMENT&sourceId=2301393.1&id=260449.1) Everything You Wanted to Know About the Apache-Based OHS Version  **4. Java** **的安全漏洞**  我需要更新JDK或者其它Oracle 产品用的JDK吗? 如果是应该怎样做? 维护Oracle Fusion Middleware 产品的最佳实践是什么?  **回答:**  为了保护Oracle产品不受Java的安全漏洞影响，您应该保持更新Critical Patch Update(CPU)包含的Java SE或者JDK 和 JRE的补丁。每个季度发布的安全建议包含Java SE、Oracle Fusion Middleware和Oracle Database产品。你应该参考 CVE 和风险评估表并决定对你的应用采取适当的行动。当需要更新Java SE版本时一定要遵循Oracle 产品认证文档。请参考下面的文档。  [Note 1492980.1](https://support.oracle.com/epmos/faces/DocumentDisplay?parent=DOCUMENT&sourceId=2301393.1&id=1492980.1) How to Maintain the Java SE Installed or Used with FMW 11g/12c Products  [Note 1506916.1](https://support.oracle.com/epmos/faces/DocumentDisplay?parent=DOCUMENT&sourceId=2301393.1&id=1506916.1) Obtaining Java SE (JDK/JRE) for Oracle Fusion Middleware Products  [Note 952075.1](https://support.oracle.com/epmos/faces/DocumentDisplay?parent=DOCUMENT&sourceId=2301393.1&id=952075.1) Java SE (J2SE) End of Life and Oracle Fusion Middleware Policy  Additional Keywords:    CVE-2014-3566 CVE-2014-6271 CVE-2014-7169 CVE-2014-0160 track xss cross site cross-site scripting scanner Nessus Qualys Dranzer mod\_security secfilter attack injection javascript expect header Retina Rational AppScan CVE-2010-4476 CVE 2010-4476 sql injection  **参考**  [NOTE:944866.1](https://support.oracle.com/epmos/faces/DocumentDisplay?parent=DOCUMENT&sourceId=2301393.1&id=944866.1) - Error Correction Support Dates for Oracle Fusion Middleware (10g/11g/12c/WLS)  [NOTE:1070309.1](https://support.oracle.com/epmos/faces/DocumentDisplay?parent=DOCUMENT&sourceId=2301393.1&id=1070309.1) - SR Creation Tips for Oracle Application Server and Oracle Fusion Middleware Core/Install Type of Issues |