

Oracle® Solaris Studio 12.4: Sicherheitshandbuch



Teilenr.: E60508
Oktober 2014

Copyright © 2013, 2014, Oracle und/oder verbundene Unternehmen. All rights reserved. Alle Rechte vorbehalten.

Diese Software und zugehörige Dokumentation werden im Rahmen eines Lizenzvertrages zur Verfügung gestellt, der Einschränkungen hinsichtlich Nutzung und Offenlegung enthält und durch Gesetze zum Schutz geistigen Eigentums geschützt ist. Sofern nicht ausdrücklich in Ihrem Lizenzvertrag vereinbart oder gesetzlich geregelt, darf diese Software weder ganz noch teilweise in irgendeiner Form oder durch irgendein Mittel zu irgendeinem Zweck kopiert, reproduziert, übersetzt, gesendet, verändert, lizenziert, übertragen, verteilt, ausgestellt, ausgeführt, veröffentlicht oder angezeigt werden. Reverse engineering, Disassemblieren bzw. Dekompilieren dieser Software ist verboten, es sei denn dies ist zur Interoperabilität gesetzlich gestattet.

Die hier angegebenen Informationen können jederzeit und ohne vorherige Ankündigung geändert werden. Wir übernehmen keine Gewähr für deren Richtigkeit. Sollten Sie Fehler oder Unstimmigkeiten finden, bitten wir Sie, uns diese schriftlich mitzuteilen.

Wird diese Software oder zugehörige Dokumentation an die Regierung der Vereinigten Staaten von Amerika bzw. einen Lizenznehmer im Auftrag der Regierung der Vereinigten Staaten von Amerika geliefert, gilt Folgendes:

U.S. GOVERNMENT END USERS. Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

Diese Software oder Hardware ist für die allgemeine Anwendung in verschiedenen Informationsmanagementanwendungen konzipiert. Sie ist nicht für den Einsatz in potenziell gefährlichen Anwendungen bzw. Anwendungen mit einem potenziellen Risiko von Personenschäden geeignet. Falls die Software oder Hardware für solche Zwecke verwendet wird, verpflichtet sich der Lizenznehmer, sämtliche erforderlichen Maßnahmen wie Fail Safe, Backups und Redundancy zu ergreifen, um den sicheren Einsatz dieser Software oder Hardware zu gewährleisten. Oracle Corporation und ihre verbundenen Unternehmen übernehmen keinerlei Haftung für Schäden, die beim Einsatz dieser Software oder Hardware in gefährlichen Anwendungen entstehen.

Oracle und Java sind eingetragene Marken von Oracle und/oder ihren verbundenen Unternehmen. Andere Namen und Bezeichnungen können Marken ihrer jeweiligen Inhaber sein.

Intel und Intel Xeon sind Marken oder eingetragene Marken der Intel Corporation. Alle SPARC-Marken werden unter Lizenz verwendet und sind Marken oder eingetragene Marken von SPARC International Inc. AMD, Opteron, das AMD-Logo und das AMD-Opteron-Logo sind Marken oder eingetragene Marken von Advanced Micro Devices. UNIX ist eine eingetragene Marke von The Open Group.

Diese Software oder Hardware und die zugehörige Dokumentation können Zugriffsmöglichkeiten auf Inhalte, Produkte und Serviceleistungen von Dritten enthalten. Oracle Corporation und ihre verbundenen Unternehmen übernehmen keine Verantwortung für Inhalte, Produkte und Serviceleistungen von Dritten und lehnen ausdrücklich jegliche Art von Gewährleistung diesbezüglich ab. Oracle Corporation und ihre verbundenen Unternehmen übernehmen keine Verantwortung für Verluste, Kosten oder Schäden, die aufgrund des Zugriffs oder der Verwendung von Inhalten, Produkten und Serviceleistungen von Dritten entstehen.

Inhalt

- Verwenden dieser Dokumentation 5**
- 1 Oracle Solaris Studio-Sicherheitsinformationen 7**
 - Oracle Solaris Studio-Sicherheitsgesichtspunkte 7
 - Vorsichtsmaßnahmen für Systemadministratoren und Benutzer, die Oracle Solaris Studio installieren 8
 - Vorsichtsmaßnahmen für Entwickler 8
 - Verwenden von Oracle Solaris Studio-Bibliotheken 8
 - Verwenden der Remote-Entwicklung in IDE 9
 - Verwenden von Remote-Entwicklung in Performance Analyzer 9

Verwenden dieser Dokumentation

- **Überblick** - Beschreibt Sicherheitsprobleme, über die Benutzer bei diesem Oracle Solaris Studio 12.4-Release informiert sein müssen.
- **Zielgruppe** – Anwendungsentwickler, Systementwickler, Architekten, Supporttechniker
- **Vorkenntnisse** – Programmiererfahrung, Testen von Softwareentwicklungen, Erfahrung bei Generieren und Kompilieren von Softwareprodukten

Produktdokumentationsbibliothek

Dokumentation, neueste Informationen und bekannte Probleme für dieses Produkt finden Sie in der Dokumentationsbibliothek unter http://docs.oracle.com/cd/E37069_01.

Die bekannten Probleme für dieses Oracle Solaris Studio-Release finden Sie im Kapitel „Known Problems, Limitations, and Workarounds in This Release“ in „Oracle Solaris Studio 12.4: Release Notes“. Weitere Informationen zu Compilern und Tools finden Sie in den entsprechenden Manpages oder der Hilfe.

Kontakt zu Oracle Support

Oracle-Kunden können über My Oracle Support den Onlinesupport nutzen. Informationen dazu erhalten Sie unter <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> oder unter <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> (für Hörgeschädigte).

Feedback

Unter <http://www.oracle.com/goto/docfeedback> können Sie uns Feedback zu dieser Dokumentation geben.

Oracle Solaris Studio-Sicherheitsinformationen

Dieses Dokument umfasst Informationen zu:

- „Oracle Solaris Studio-Sicherheitsgesichtspunkte“ [7]
- „Vorsichtsmaßnahmen für Systemadministratoren und Benutzer, die Oracle Solaris Studio installieren“ [8]
- „Vorsichtsmaßnahmen für Entwickler“ [8]
- „Verwenden von Oracle Solaris Studio-Bibliotheken“ [8]
- „Verwenden der Remote-Entwicklung in IDE“ [9]
- „Verwenden von Remote-Entwicklung in Performance Analyzer“ [9]

Oracle Solaris Studio-Sicherheitsgesichtspunkte

Oracle Solaris Studio besteht aus einer Suite von Compilern, Debuggern und Analysetools sowie IDE (Integrated Development Environment) für Entwicklung, Debugging und Optimierung von Anwendungen für die Solaris- und Linux-Plattformen. Wie andere Entwicklungstools sind die Oracle Solaris Studio-Compiler und -Tools zur Verwendung in einer Umgebung ausgelegt, die von Production-Umgebungen isoliert ist, weil Benutzer auf diese Tools zugreifen können, um Anwendungen während der Ausführung zu manipulieren. Weil Production-Umgebungen im Allgemeinen im Fokus der Sicherheitserwägungen liegen, müssen Entwicklertools und Entwicklungsumgebungen auch unter einem Sicherheitsaspekt betrachtet werden.

Systemadministratoren spielen eine wichtige Rolle bei der Festlegung der Assets, die geschützt werden müssen, und beim Einsatz von Steuerelementen und Policies zum Schutz dieser Assets. Oracle Solaris Studio alleine ermöglicht keinen Zugriff auf Assets oder Features der Betriebsumgebung, die der Benutzer noch nicht hat. Bei Oracle Solaris Studio besteht das Risiko, dass Benutzer, die unberechtigten Zugriff auf Assets oder Systeme auf Wegen erhalten haben, die Oracle Solaris Studio nicht einschließen, die Funktionen der Oracle Solaris Studio-Entwicklertools nutzen und so eine Sicherheitslücke verursachen können. Ein Benutzer, der die Oracle Solaris Studio-Tools ausführt, hat Zugriff zu allen Funktionen, die Debugger und Analysten direkt über die Betriebssystemschnittstellen nutzen. Mit den Oracle Solaris Studio-Tools können diese Betriebssystemfunktionen jedoch einfacher verstanden und verwendet werden, um die Interna von Anwendungen zu testen, Hardwareregistrierungen, Speicher und Stack zu manipulieren und die Ausführung einer Anwendung zu kontrollieren.

Vorsichtsmaßnahmen für Systemadministratoren und Benutzer, die Oracle Solaris Studio installieren

Oracle Solaris Studio-Compiler und -Tools sind in erster Linie zur Verwendung in Entwicklungsumgebungen gedacht. Wenn Oracle Solaris Studio in einer Production-Umgebung benötigt wird (z.B. um eine Production-Anwendung zu debuggen oder einen Performanceengpass zu analysieren), müssen Maßnahmen ergriffen werden, um den Zugriff auf diese Tools zu begrenzen. Installieren Sie nur die Oracle Solaris Studio-Komponenten, die für Entwicklungs- oder Production-Aufgaben benötigt werden. Bei dem Installationsprogramm für das Oracle Solaris Studio-Package können Sie wählen, welche Studio-Komponenten installiert werden sollen.

Mit Oracle Solaris Studio-IDE können Sie nicht von Oracle stammende Plug-ins installieren, die unterstützt werden. Bevor Sie Software von Fremdherstellern herunterladen, wie diese Plug-ins, prüfen Sie die Sicherheitsrisiken dieser Plug-ins.

Halten Sie Installationen von Oracle Solaris Studio mit den neuesten Patches, insbesondere Sicherheitspatches, auf dem neuesten Stand.

Oracle Solaris Studio Performance Analyzer erfordert höhere Berechtigungen für bestimmte Debugging- und Analyseaufgaben. Stellen Sie diese Berechtigungen über temporäre Accounts bereit, und überwachen Sie diese Accounts entsprechend.

Vorsichtsmaßnahmen für Entwickler

Oracle Solaris Studio-Compiler und -Tools erstellen Ausgabedateien, wie Logs, Core-Dumps und Objektdaten. Die Berechtigungen für diese Dateien werden mit den Standardberechtigungen des Benutzers festgelegt. Um die Ausgabedateien vor unerwünschtem Zugriff zu schützen, begrenzen Sie die Standardberechtigungen, sodass nur der unbedingt erforderliche Zugriff gewährt wird. Benutzer legen die Standardberechtigungen mit dem Solaris- und Linux-Befehl `umask` fest.

Verwenden von Oracle Solaris Studio-Bibliotheken

Oracle Solaris Studio umfasst ein Set von Bibliotheken, die Unterstützung für unterstützte Plattformen zur Laufzeit bieten: Performancebibliotheken für rechenintensive Anwendungen sowie Debugging- und Performanceanalysebibliotheken zur Optimierung von Anwendungen in einer Entwicklungsumgebung. Performance- und Laufzeitbibliotheken werden in Production-Umgebungen verwendet und werden nach Bedarf von Systemadministratoren für die Anwendungen installiert, die ausgeführt werden.

Wie der Name sagt, sind Performancebibliotheken für Performance optimiert, d.h. die Datenprüfung wird auf ein Mindestmaß beschränkt, um maximale Performance zu gewährleisten. Bei der Verwendung von Performancebibliotheken ist der Anwendungsentwickler für die Validierung von Daten verantwortlich, die an diese Bibliotheken übergeben werden.

Verwenden der Remote-Entwicklung in IDE

Die Verwendung von Remote Build-Hosts in IDE erfordert Anmeldezugangsdaten. Beeinträchtigte Sicherheit auf dem Clientsystem, auf dem IDE ausgeführt wird, könnte zu nicht autorisiertem Zugriff der Remote-Serverhosts führen. In freigegebenen Desktopumgebungen wird von der Speicherung von Anmeldezugangsdaten in Fällen abgeraten, die ein hohes Maß an Sicherheit erfordern.

Ein weiterer Bereich, der bei der Remote-Entwicklung beachtet werden muss, ist das Caching von Quellcode auf Clientsystemen während der Remote-Entwicklung. Um die IDE-Performance und -Reaktion zu erhöhen, cacht das Remote-Entwicklungsfeature in IDE die Dateien vom Server, einschließlich Quellcode, auf dem Clientrechner. Der Cacheordner auf dem Clientrechner ist `user_directory/var/cache/remote-files`.

Bei Solaris- und Linux-Plattformen ist `user_directory`: `~/.solstudio/ide-Version-BS--Architektur` (Beispiel: `~/.solstudio/ide-12.4-SunOS-i386`).

Bei Microsoft Windows-Plattformen ist `user_directory`: `~/Application Data/.solstudio/dd-Version`.

Bei Mac OS X-Plattformen ist `user_directory`: `~/Library/Application/Support/solstudio/dd-Version`.

Gehen Sie in sensiblen Sicherheitsumgebungen vorsichtig mit diesem Cacheordner um, einschließlich Löschen und Verschlüsseln.

Verwenden von Remote-Entwicklung in Performance Analyzer

Der Remote-Client von Performance Analyzer erfordert einen Benutzernamen und ein Kennwort für die Anmeldung bei dem Remote-Server. Der Benutzername wird auf dem Datenträger im Home-Verzeichnis des Benutzers gespeichert, das Kennwort wird jedoch nie auf dem Datenträger gespeichert.

Der Remote-Client von Performance Analyzer verwendet eine Java-Implementierung von `ssh` (jssh Version 0.1.49) für die Verbindung zu dem `sshd`-Server auf dem Remote-Host.

Der Performance Analyzer-Client speichert Informationen in der Datei `~/.solstudio/analyzer-12.4/analyzer.xml` auf allen Clientplattformen einschließlich Oracle Solaris, Linux, MacOS und Microsoft Windows.