

Copyright (c) 2022, Oracle. All rights reserved. Oracle Confidential.

Critical Patch Update (CPU) Program Jul 2022 Patch Availability Document (DB-only) (Doc ID 2867871.1)

APPLIES TO:

Oracle Database Cloud Exadata Service - Version N/A and later
Oracle Database - Standard Edition - Version 12.1.0.2 and later
Oracle Database Cloud Service - Version N/A and later
Oracle Database Exadata Express Cloud Service - Version N/A and later
Oracle Database - Enterprise Edition
Information in this document applies to any platform.

PURPOSE

This document defines the patches and minimum releases for the Database Product Suite Critical Patch Updates and Patch Set Updates released on July 19, 2022.

SCOPE

The document is for Database Administrators and/or others tasked with Quarterly Security Patching.

DETAILS

Critical Patch Update Program Jul 2022 Patch Availability Document (DB-only)

My Oracle Support [Note 2867871.1](#)

Released July 19, 2022

This document contains the following sections:

- [Critical Patch Update July 2022 Patch Availability Document \(PAD\)](#)
 - [1 Overview](#)
 - [1.1 How To Use This Document](#)
 - [1.2 Terminology in the Tables](#)
 - [1.3 On-Request Patches](#)
 - [1.4 CPU Program and My Oracle Support Patch Recommendations](#)
 - [1.5 My Oracle Support \(MOS\) Conflict Checker Tool](#)
 - [2 What's New in July 2022](#)
 - [2.1 "Final CPU Information \(Error Correction Policies\)"](#)
 - [2.2 "Post Release Patches"](#)
 - [2.3 "Separate PADs for Separate Products"](#)
 - [3 Patch Availability for Oracle Products](#)
 - [3.1 Oracle Database](#)
 - [3.2 Oracle Sun Middleware](#)
 - [3.3 Tools](#)
 - [4 Final CPU History](#)
 - [5 Sources of Additional Information](#)
 - [6 Modification History](#)
 - [7 Documentation Accessibility](#)

Quick Links: [Read Me First](#) [DB 19c](#)

1 Overview

Oracle provides quarterly cumulative patches to address security vulnerabilities. The patches may include critical fixes in addition to the security fixes. The security vulnerabilities addressed are announced in the Advisory for July 2022, available at:

[Oracle Technical Network Advisory](#)

This document lists the Oracle Database CPU program cumulative patches for product releases under error correction. The July 2022 release supersedes earlier CPU program cumulative patches for the same product releases. This document is subject to continual update after the initial release, and the changes are listed in "[Modification History](#)." If you print this document, check My Oracle Support to ensure you have the latest version.

This section contains the following:

- [Section 1.1 "How To Use This Document"](#)
- [Section 1.2 "Terminology in the Tables"](#)
- [Section 1.3 "On-Request Patches"](#)
- [Section 1.4 "CPU Program and My Oracle Support Patch Recommendations"](#)
- [Section 1.5 "My Oracle Support \(MOS\) Conflict Checker Tool"](#)

1.1 How To Use This Document

The following steps explain how to use this document.

Step 1 Assess your Environments

Determine the Oracle product suites and products and their release numbers for each of your environments.

Step 2 Read Important Announcements

Review "[What's New in July 2022](#)," as it lists documentation and packaging changes along with important announcements such as upcoming final CPUs.

Step 3 Determine Patches to be Applied

For each environment, determine which patches need to be applied by using the tables in "[Patch Availability for Oracle Products](#)." There is one availability table for each product suite release, such as Oracle Database 19c.

- The table lists the patches to be applied either to the product or to the appropriate product Oracle homes that are associated with the product suite
- The patches are listed in the order released, with newest patches listed first
- For some patches, multiple Oracle homes are listed. Apply the patch to all of the homes indicated that are applicable to your environment and only to the listed Oracle homes
- The table lists only product releases that are under Premier Support or Extended Support and are under error correction as defined in My Oracle Support [Note 209768.1](#), *Database, FMW, Enterprise Manager, TimesTen In-Memory Database, and OCS Software Error Correction Support Policy*. Patches are provided only for these releases. If you do not see the release that you have installed, then check "[Final CPU History](#)" and contact Oracle Support for further assistance
- Patches that include security vulnerabilities announced in the current quarter's CPU Advisory, list the vulnerability CVE numbers in the Advisory Number column. If you are interested in the risk matrix for the vulnerabilities fixed in the patch, then see the CPU Advisory at <http://www.oracle.com/technetwork/topics/security/alerts-086861.html>. For patches that are listed from previous quarterly releases, or the current one without any security fixes, the column indicates "Released MMM YYYY"
- When a section is referenced in a table, follow the link to determine which patches to install. For example, when "[Oracle Database](#)" is referenced, determine the Oracle Database release that is installed, and find the patches to apply in the table for that Oracle Database release in "[Oracle Database](#)."

Step 4 Apply the Patches

Download the patches, review the READMEs, and apply the patches according to the instructions.

Step 5 Planning for Future Critical Patch Updates

To help you plan for future Critical Patch Updates, this document includes Final CPU information based on Oracle's Lifetime Support Policy and error correction policies.

"[Final CPU Information \(Error Correction Policies\)](#)" in "[What's New in July 2022](#)," documents product releases for which final Critical Patch Updates are upcoming or are being announced. In each product section, there is also an Error Correction Information Table that documents the final CPU program patch for the product. Products that have reached the end of error correction are documented in "[Final CPU History](#)."

Oracle recommends that you [subscribe](#) to this Patch Availability Document in order to stay informed of any emergent problems.

1.2 Terminology in the Tables

The following terminology is used in this patch availability document and in the subsequent tables.

- **Update (RU)** - Release Update
- **Revision (RUR)** -Release Update Revision
- **BP** - Bundle Patch
- **Final CPU** is the last quarter that a product is supported in the CPU program as per the Premier Support and Extended Support policies. <http://www.oracle.com/us/support/lifetime-support/index.html>.
- **NA** Not Applicable.
- **OR** On-Request. The patch is made available through the On-Request program.
- **PSU** - Patch Set Update
- **SPU** - Security Patch Update. An iterative, cumulative patch consisting of security fixes.
- **Overlay SPU** patch provided as an overlay on top of a PSU or BP instead of a base/patch set release.

1.3 On-Request Patches

Oracle does not proactively release patches for historically inactive platforms. However, Oracle will deliver these patches when requested.

The following guidelines describe how to initiate an on-request (OR) patch.

A request may be made:

- At any time. However, a patch for a specific quarterly release, such as CPUOct2019, cannot be requested. Depending on when the request is received and processed, either the patch for the current quarterly release or the next quarterly release will be provided. Your Service Request (SR) will provide you the planned availability date for the patch.
- As long as the version is in either Premier Support or Extended Support and error correction support has not expired. For example, if a product release is under Extended Support through the release of CPUJan2020 on January 15, 2020, then you can file a request for the product release through January 29, 2020. For more information, see [Oracle Lifetime Support Policies](#) at <http://www.oracle.com/us/support/lifetime-support/index.html>, and [Note 209768.1](#), *Database, FMW, Enterprise Manager, TimesTen In-Memory Database, and OCS Software Error Correction Support Policy*.
- For a platform-version combination when a major release or patch set is released on a platform after a quarterly release date. Oracle will provide the next patch for that platform-version combination, however you may request the current patch by following the on-request process. For example, if a patch is released for a platform on August 1, 2020, Oracle will provide the CPUOct2020 patch for that platform. You may request a CPUOct2020 patch for the platform, and Oracle will review the request and determine whether to provide CPUJul2020 or CPUOct2020.

A patch that is marked as on-request (OR) may already have been requested by another customer and be available on My Oracle Support. Before you file a Service Request (SR), check on My Oracle Support to see if the patch is already available for your platform.

1.4 CPU Program and My Oracle Support Patch Recommendations

My Oracle Support patch recommendation features are available on the Patches & Update tab. The patches announced in this document as part of the CPU program are classified as "Security" patch recommendations in My Oracle Support. If a new patch is being announced in this document, then the classification on any earlier patch is changed to "General", causing it to be removed from the My Oracle Support patch recommendations. If a patch has a "Security" classification, and a subsequent bundle, SPU, or PSU is released with a recommendation classification, then it will be classified as a "Security" recommendation in My Oracle Support.

Once a product release is no longer in error correction, its CPU patch information is removed from this document, but the last patch recommendation continues to be available in My Oracle Support. Ensure to select each of the products installed in your environment to obtain all patches.

1.5 My Oracle Support (MOS) Conflict Checker Tool

The My Oracle Support (MOS) Conflict Checker tool is available as of July 21, 2014.

You can access MOS Conflict Checker at <https://support.oracle.com/epmos/faces/PatchConflictCheck>. This tool is also accessible from the Patch Search results screen ("Analyze with OPatch" button).

The MOS Conflict Checker Tool allows you to upload an OPatch inventory to check for conflicts with patches to apply to your environment. If no conflicts are found, you can download the patches. If conflicts are found, the tool finds an existing resolution to download. If no resolution is found, you can request a solution, and monitor your request in the Plans region.

For more information and a demonstration video, see Knowledge Document [Note 1091294.1](#), *How to Use the My Oracle Support Conflict Checker Tool for Patches Installed with OPatch [Video]*.

2 What's New in July 2022

This section describes important changes in July 2022:

- [Section 2.1 "Final CPU Information \(Error Correction Policies\)"](#)
- [Section 2.2 "Post Release Patches"](#)
- [Section 2.3 "Separate PADs for Separate Products"](#)

2.1 Final CPU Information (Error Correction Policies)

The final CPU is the last quarter that a product is supported in the CPU program as per the Premier Support and Extended Support policies. Final CPUs for upcoming releases, as well as newly scheduled final CPUs, are listed in the following sections.

Final CPUs scheduled for Jul 2022

- Oracle GoldenGate Monitor 12.1.3.x
- Oracle GoldenGate Veridata 12.1.3

Final CPUs scheduled for Oct 2022

- Oracle Directory Server Enterprise Edition 11.1.1.7.0

2.2 Post Release Patches

Oracle strives to complete preparations and testing of each Quarterly Security Patch for each platform by the quarterly release date. Occasionally, circumstances beyond our control dictate that a particular patch be delayed and be released a few days after the quarterly release date. The following table lists any current patch delays and the estimated date of availability.

Oracle GoldenGate 19.1.0.0.220719 for Oracle 11g [Patch 34377350](#) Linux x86-64, Solaris Sparc64, AIX Available

Patch	Patch Number	Platform	Availability
Oracle GoldenGate 21.7.0.0.0	Patch 34315141	Linux x86-64, Windows x64	Available

Microservices for Oracle			
Oracle GoldenGate 21.7.0.0.0 for Oracle	Patch 34315139	Linux x86-64, Windows x64	Available
Oracle GoldenGate 19.1.0.0.220719 for Oracle 12c	Patch 34377368	Linux x86-64, Solaris Sparc64, AIX	Available
Oracle GoldenGate 19.1.0.0.220719 for Oracle 18c	Patch 34377377	Linux x86-64, Solaris Sparc64, AIX	Available
Oracle GoldenGate 19.1.0.0.220719 for Oracle 19c	Patch 34377379	Linux x86-64, Solaris Sparc64, AIX	Available
19.15.1.0.220719 DB RUR	Patch 34119532	Linux x86-64	Available
		Solaris Sparc64, Solaris x86-64, zLinux, HP-UX Itanium, AIX	12-Aug-2022
19.15.1.0.220719 GI RUR	Patch 34110582	Linux x86-64	Available
		Solaris Sparc64, Solaris x86-64, zLinux, HP-UX Itanium, AIX	12-Aug-2022
19.14.2.0.220719 DB RUR	Patch 34110559	Linux x86-64	Available
		Solaris Sparc64, Solaris x86-64, zLinux, HP-UX Itanium, AIX	12-Aug-2022
19.14.2.0.220719 GI RUR	Patch 34164837	Linux x86-64	Available
		Solaris Sparc64, Solaris x86-64, zLinux, HP-UX Itanium, AIX	12-Aug-2022
12.1.0.2.220719 Proactive DBBP	Patch 34204559	Linux x86-64	Available
COMBO 12.1.0.2.220719 Proactive DBBP	Patch 34163651	Linux x86-64	Available
12.1.0.2.220719 Proactive DBBP (& associated COMBO)	Patch 34204559 (& Patch 34163651)	Solaris Sparc64, Solaris x86-64, zLinux, HP-UX Itanium, AIX	12-Aug-2022
12.1.0.2.220719 DBPSU	Patch 34057742	Linux x86-64	Available
COMBO 12.1.0.2.220719 DBPSU	Patch 34163630	Linux x86-64	Available
12.1.0.2.220719 DBPSU (& associated COMBO)	Patch 34057742 (& Patch 34163630)	Solaris Sparc64, Solaris x86-64, zLinux, HP-UX Itanium, AIX	12-Aug-2022
12.1.0.2.220719 GIPSU	Patch 34204576	Linux x86-64	Available
COMBO 12.1.0.2.220719 GIPSU	Patch 34163645	Linux x86-64	Available
12.1.0.2.220719 GIPSU (& associated COMBO)	Patch 34204576 (& Patch 34163645)	Solaris Sparc64, Solaris x86-64, zLinux, HP-UX Itanium, AIX	12-Aug-2022
OJVM Release Update 19.16.0.0.220719	Patch 34086870	MS-Windows	Available
21.7.0.0.220719 WIN BP	Patch 34110698	MS-Windows	12-Aug-2022
19.16.0.0.220719 WIN BP	Patch 34110685	MS-Windows	Available
12.1.0.2.220719 WIN BP	Patch 33883271	MS-Windows	Available
Quarterly Full Stack download for Exadata (Jul2022) 21.7.0	Patch 34206020	All	12-Aug-2022
Quarterly Full Stack download for Exadata (Jul2022) 19.16.0	Patch 34206004	All	12-Aug-2022
Quarterly Full Stack download for Exadata (Jul2022) 12.1.0.2	Patch 34205981	All	12-Aug-2022
Quarterly Full Stack download for SuperCluster (Q3.2022)	Patch 34206024	All	06-Sep-2022

Oracle recommends that you [subscribe](#) to this PAD NOTE in order to stay informed of any emergent updates.

2.3 Separate PADs for Separate Products

In response to Oracle Customer requests for a shorter and easier to use PAD, the following Oracle Products have each been localized into their own, product-specific PAD:

- Oracle Database, this document
- Oracle Enterprise Manager, [Note 2867874.1](#)
- Oracle Hyperion, [Note 2775466.2](#)
- Oracle Fusion Middleware, [Note 2853458.2](#)
- Oracle Analytics, [Note 2853459.2](#)

This change was implemented beginning in the April 2022 quarter.

3 Patch Availability for Oracle Products

This section contains the following:

- [Section 3.1 "Oracle Database"](#)
- [Section 3.2 "Oracle Sun Middleware"](#)
- [Section 3.3 "Tools"](#)

3.1 Oracle Database

This section contains the following:

- [Section 3.1.1 "Oracle REST Data Services \(formally called Oracle APEX Listener\)"](#)
- [Section 3.1.2 "Oracle Application Express"](#)
- [Section 3.1.3 "Oracle Autonomous Health Framework \(TFA and ORACHK/EXACHK\)"](#)
- [Section 3.1.4 "Oracle Blockchain Platform - Enterprise Edition"](#)
- [Section 3.1.5 "Oracle Graph Server and Client"](#)
- [Section 3.1.6 "Oracle Big Data Spatial and Graph"](#)
- [Section 3.1.7 "Oracle Database"](#)
- [Section 3.1.8 "Oracle Database Mobile/Lite Server"](#)
- [Section 3.1.9 "Oracle GoldenGate"](#)
- [Section 3.1.10 "Oracle GoldenGate for Big Data \(Formerly known as Oracle GoldenGate Application Adapters\)"](#)
- [Section 3.1.11 "Oracle GoldenGate Monitor"](#)
- [Section 3.1.12 "Oracle GoldenGate Veridata"](#)
- [Section 3.1.13 "Oracle NoSQL Database"](#)
- [Section 3.1.14 "Oracle Secure Backup"](#)
- [Section 3.1.15 "Oracle Spatial Studio"](#)
- [Section 3.1.16 "Oracle SQL Developer"](#)
- [Section 3.1.17 "Oracle Stream Analytics"](#)
- [Section 3.1.18 "Oracle TimesTen In-Memory Database"](#)
- [Section 3.1.19 "Oracle Essbase"](#)

3.1.1 Oracle REST Data Services (formally called Oracle APEX Listener)

Minimum Product Requirements for Oracle REST Data Services

Critical Patch Update security vulnerabilities are fixed in the listed releases. For Oracle REST Data Services downloads and installation instructions, see <http://www.oracle.com/technetwork/developer-tools/rest-data-services/overview/index.html>.

Product	Release	Advisory Number	Comments
Oracle REST Data Services	22.2	CVE-2021-34429, CVE-2021-41184, CVE-2021-41183, and CVE-2021-41182	

3.1.2 Oracle Application Express

Minimum Product Requirements for Oracle Application Express

Critical Patch Update security vulnerabilities are fixed in the listed releases. For Oracle Application Express downloads and installation instructions, see <http://www.oracle.com/technetwork/developer-tools/apex/downloads/index.html>.

Component	Release	Advisory Number	Comments
Oracle Application Express	22.1.0 Bundle Patch or later	CVE-2022-24729, CVE-2022-24728, CVE-2021-41184, CVE-2021-41182, and CVE-2021-41183	

3.1.3 Oracle Autonomous Health Framework (TFA and ORACHK/EXACHK)

Minimum Product Requirements for Autonomous Health Framework

Critical Patch Update security vulnerabilities are fixed in the listed releases. For Autonomous Health Framework downloads and installation instructions, see [Note 2550798.1](#), "Autonomous Health Framework (AHF) - Including TFA and ORAchK/EXAchK"

Component	Release	Advisory Number	Comments
Autonomous Health Framework	AHF 22.1.0 Release. See MOS Note 2550798.1 to download patch	CVE-2021-41496, CVE-2021-41495, CVE-2021-29921, CVE-2020-29396, CVE-2020-36518	Autonomous Health Framework (AHF) - Including TFA and ORAchK/EXAchK Note 2550798.1

3.1.4 Oracle Blockchain Platform - Enterprise Edition

Minimum Product Requirements for Oracle Blockchain Platform - Enterprise Edition

Critical Patch Update security vulnerabilities are fixed in the listed releases. For Oracle Blockchain Platform - Enterprise Edition downloads and installation instructions, see <https://www.oracle.com/blockchain/blockchain-platform-enterprise-edition/>.

Component	Release	Advisory Number	Comments
Oracle Blockchain Platform - Enterprise Edition	21.1.2	Released April 2022	
Oracle Blockchain Platform - Enterprise Edition	Hotfix for OBPEE 21.1.2 Patch 33795456	Released April 2022	

3.1.5 Oracle Graph Server and Client

Minimum Product Requirements for Oracle Graph Server and Client

Critical Patch Update security vulnerabilities are fixed in the listed releases. For Oracle Graph Server and Client downloads and installation instructions, see <https://www.oracle.com/database/technologies/spatialandgraph/property-graph-features/graph-server-and-client/graph-server-and-client-downloads.html>

Component	Release	Advisory Number	Comments
Oracle Graph Server and Client	22.2	CVE-2020-36518, CVE-2022-23181, CVE-2020-9484	For more information on Log4j Vulnerabilities, see Note 2827611.1 For more information on CVE-2021-44228, see Note 2828603.1

3.1.6 Oracle Big Data Spatial and Graph

Minimum Product Requirements for Oracle Big Data Spatial and Graph

Critical Patch Update security vulnerabilities for the graph feature of Oracle Big Data Spatial and Graph are fixed in the listed releases. For downloads and installation instructions, see <https://www.oracle.com/database/technologies/spatialandgraph/property-graph-features/graph-server-and-client/graph-server-and-client-downloads.html>

Component	Release	Advisory Number	Comments
Big Data Spatial and Graph	Oracle Graph Server and Client 22.2 (released April 2022) should replace all installations of graph feature of Oracle Big Data Spatial and Graph	CVE-2021-42340, CVE-2021-41182, CVE-2021-41183, CVE-2021-41184, CVE-2020-36518	Steps to replace BDSG 3.0 and all prior installations with Oracle Graph Server and Client 22.2: (1) Apply Patch 33695304 to remove all BDSG bits. (2) If using Graph feature of Big Data Spatial and Graph, download and use Graph Server and Client 22.2 by downloading from https://www.oracle.com/database/technologies/spatialandgraph/property-graph-features/graph-server-and-client/graph-server-and-client-downloads.html or Oracle Software Delivery Cloud. The Oracle Graph HDFS Connector component contains the libraries to connect Oracle Graph with Apache Hadoop Distributed Filesystem (HDFS).

3.1.7 Oracle Database

This section contains the following:

- [Section 3.1.7.1 "Patch Availability for Oracle Database"](#)
- [Section 3.1.7.2 "Oracle Database 21"](#)
- [Section 3.1.7.3 "Oracle Database 19"](#)
- [Section 3.1.7.4 "Oracle Database 12.1.0.2"](#)

3.1.7.1 Patch Availability for Oracle Database

For information regarding the different types of patches for Database, refer to Oracle Database - Overview of Database Patch Delivery Methods - 12.1.0.2 and older, [Note 1962125.1](#) and Oracle Database - Overview of Database Patch Delivery Methods for 12.2.0.1 and greater, [Note 2337415.1](#)

3.1.7.2 Oracle Database 21

Patch Information	21	Comments
Final CPU	See Note 742060.1	

On-Request platforms	32-bit client-only platforms	
----------------------	------------------------------	--

Patch Availability for Oracle Database 21

Product Home	Patch	Advisory Number	Comments
Oracle Database Server home	Database Release Update 21.7.0.0.220719 Patch 34160444 for UNIX, or GI Release Update 21.7.0.0.220719 Patch 34155589 , or Microsoft Windows 32-Bit and x86-64 BP 21.7.0.0.220719 Patch 34110698 or later, or Quarterly Full Stack download for Exadata (Jul2022) 21.7.0 Patch 34206020 for Linux x86-64, or	CVE-2021-45943, CVE-2022-21432, CVE-2020-26185, CVE-2020-26184, CVE-2022-21565, CVE-2020-35169	21c does not have COMBO nor OJVM patches. Instead, the OJVM fixes are contained within the DB RU and the GI RU patches. The Database and GI Update and Revision patches include the JDK fixes released in the prior cycle. For the most recent JDK fixes a separate patch is available (see below) and needs to be installed in addition to the Database and GI patches. For patch availability, see section 2.2 Post Release Patches
Oracle Database Server, Gateway, Client and Global Data Services Home	JDK8u341 Patch 34113643	CVE-2022-34169, CVE-2022-21541, CVE-2022-21540	See Note 2584628.1 , "JDK and PERL Patches for Oracle Database Home and Grid Home" for information on availability and prior patches. JDK patches for 32 bit clients would be build on demand basis.
Database Server, Client, and Global Data Services Home	Perl Patch 33928944	Released April 2022	See Note 2584628.1 , "JDK and PERL Patches for Oracle Database Home and Grid Home" for information on availability and prior patches.
Oracle Database Client, Gateway, and Global Data Services Home	Database Release Update 21.7.0.0.220719 Patch 34160444 for UNIX	CVE-2020-26185, CVE-2020-26184	The Instant Client installation is not the same as the client-only Installation. For additional information about Instant Client installations, see Oracle Call Interface Programmer's Guide .

3.1.7.3 Oracle Database 19

Patch Information	19	Comments
Final CPU	See Note 742060.1	
On-Request platforms	32-bit client-only platforms	

Patch Availability for Oracle Database 19

Product Home	Patch	Advisory Number	Comments
Oracle Database	Combo OJVM Release Update	CVE-2021-45943, CVE-2022-21432, CVE-2022-0839,	See Note 1929745.1 , Oracle Recommended Patches -- Oracle JavaVM Component Database PSU (OJVM PSU) Patches.

Server home	<p>19.16.0.0.220719 and Database Release Update 19.16.0.0.220719 Patch 34160831 for UNIX, or</p> <p>Combo OJVM Release Update 19.16.0.0.220719 and GI Release Update 19.16.0.0.220719 Patch 34160854, or</p> <p>Quarterly Full Stack download for Exadata (Jul2022) 19.16.0 Patch 34206004 for Linux x86-64</p>	<p>CVE-2020-26185, CVE-2022-21565, CVE-2020-26184, CVE-2020-35169</p>	<p>For patch availability, see section 2.2 Post Release Patches</p>
Oracle Database Server home	<p>Database Release Update 19.16.0.0.220719 Patch 34133642 for UNIX, or</p> <p>GI Release Update 19.16.0.0.220719 Patch 34130714, or</p> <p>Microsoft Windows 32-Bit and x86-64 BP 19.16.0.0.220719 Patch 34110685 or later, or</p> <p>Database Release Update Revision 19.15.1.0.220719 Patch 34119532 for UNIX, or</p> <p>GI Release Update Revision 19.15.1.0.220719 Patch 34110582, or</p> <p>Database Release Update Revision 19.14.2.0.220719 Patch 34110559 for UNIX, or</p> <p>GI Release Update Revision 19.14.2.0.220719 Patch 34164837, or</p> <p>Quarterly Full Stack download for Exadata (Jul2022) 19.16.0 Patch 34206004 for Linux x86-64, or</p> <p>Quarterly Full Stack download for</p>	<p>CVE-2021-45943, CVE-2022-21432, CVE-2022-0839, CVE-2020-26185, CVE-2020-26184, CVE-2020-35169</p>	<p>From Jan2020 onwards the Database and GI Update and Revision patches include the JDK fixes released in the prior cycle. For the most recent JDK fixes a separate patch is available (see below) and needs to be installed in addition to the Database and GI patches.</p> <p>From Jan2021 onwards the Database and GI Update and Revision patches include updates to the Crypto libraries. See "MES v4.1.6 to v4.5 update 18c / 19c databases (Note 2746801.1)" for more details.</p> <p>From July 2021 onwards the Database and GI Update and Revision patches introduce a number of Native Network Encryption changes to deal with vulnerability CVE-2021-2351 and prevent the use of weaker ciphers. Customers should review: "Changes in Native Network Encryption with the July 2021 Critical Patch Update" Note 2791571.1</p> <p>For patch availability, see section 2.2 Post Release Patches</p>

	SuperCluster (Q3.2022) Patch 34206024 for Solaris SPARC 64-Bit		
Oracle Database Server home	OJVM Release Update 19.16.0.0.220719 Patch 34086870 for all platforms	CVE-2022-21565	See Note 1929745.1 , Oracle Recommended Patches -- Oracle JavaVM Component Database PSU (OJVM PSU) Patches
Oracle Database Server, Gateway, Client and Global Data Services Home	JDK8u341 Patch 34113634	CVE-2022-34169, CVE-2022-21541, CVE-2022-21540	See Note 2584628.1 , "JDK and PERL Patches for Oracle Database Home and Grid Home" for information on availability and prior patches. JDK patches for 32 bit clients would be build on demand basis.
Oracle Database Server, Client, and Global Data Services Home	Perl Patch 33912872	Released April 2022	See Note 2584628.1 , "JDK and PERL Patches for Oracle Database Home and Grid Home" for information on availability and prior patches.
Oracle Database Client, Gateway, and Global Data Services Home	Database Release Update 19.16.0.0.220719 Patch 34133642 for UNIX, or Database Release Update Revision 19.15.1.0.220719 Patch 34119532 for UNIX, or Database Release Update Revision 19.14.2.0.220719 Patch 34110559 for UNIX, or Microsoft Windows 32-Bit and x86-64 BP 19.16.0.0.220719 Patch 34110685	CVE-2020-26185, CVE-2022-0839, CVE-2020-26184	The Instant Client installation is not the same as the client-only Installation. For additional information about Instant Client installations, see Oracle Call Interface Programmer's Guide .

3.1.7.4 Oracle Database 12.1.0.2

Error Correction information for Oracle Database 12.1.0.2

Patch Information	12.1.0.2	Comments
Final CPU	See Note 742060.1	
On-Request platforms	32-bit client-only platforms	

Patch Availability for Oracle Database 12.1.0.2

If the Combo patches that are listed in the first row are applied, then the patches listed in Rows 2 and 3 do not need to be applied.

Product Home	Patch	Advisory Number	Comments
Oracle Database Server home	<p>Combo OJVM PSU 12.1.0.2.220719 and Database Proactive BP 12.1.0.2.220719 Patch 34163651 for UNIX, or</p> <p>Combo OJVM PSU 12.1.0.2.220719 and Database PSU 12.1.0.2.220719 Patch 34163630 for UNIX, or</p> <p>Combo OJVM PSU 12.1.0.2.220719 and GI PSU 12.1.0.2.220719 Patch 34163645, or</p> <p>Quarterly Full Stack download for Exadata (Jul2022) 12.1.0.2 Patch 34205981, or</p> <p>Quarterly Full Stack download for SuperCluster (Q3.2022) Patch 34206024 for Solaris SPARC 64-Bit</p>	<p>CVE-2022-21511, CVE-2020-26185, CVE-2022-21432, CVE-2022-21510, CVE-2022-21565, CVE-2020-26184, CVE-2020-35169</p>	<p>OJVM PSU Patches are not RAC Rolling installable. However, NOTE 2217053.1 defines a few specific situations where the OJVM PSU patchset can be postinstalled into each database while the database remains in unrestricted "startup" mode. Refer to the NOTE for more details.</p> <p>Combos are for environments that take a single downtime to apply all patches</p> <p>See Note 1929745.1, Oracle Recommended Patches -- Oracle JavaVM Component Database PSU (OJVM PSU) Patches.</p> <p>For patch availability, see section 2.2 Post Release Patches</p>
Oracle Database Server home	<p>Database Proactive Bundle Patch 12.1.0.2.220719 Patch 34204559, or</p> <p>Database PSU 12.1.0.2.220719 Patch 34057742 for UNIX, or</p> <p>GI PSU 12.1.0.2.220719 Patch 34204576, or</p> <p>Microsoft Windows 32-Bit and x86-64 BP 12.1.0.2.220719 Patch 33883271 or later, or</p> <p>Quarterly Full Stack download for Exadata (Jul2022)</p>	<p>CVE-2022-21511, CVE-2020-26185, CVE-2022-21432, CVE-2022-21510, CVE-2020-26184, CVE-2020-35169</p>	<p>For JDK fixes a separate patch is available (see below) and needs to be installed in addition to the Database and GI patches.</p> <p>From July 2021 onwards the Database and GI Update and Revision patches introduce a number of Native Network Encryption changes to deal with vulnerability CVE-2021-2351 and prevent the use of weaker ciphers. Customers should review: "Changes in Native Network Encryption with the July 2021 Critical Patch Update" Note 2791571.1</p> <p>From January 2022 onward the Database and GI Bundles include Security fixes to the DELL MES Security libraries used by the Database Product. Customers on AIX 6.1 should review My Oracle Support Note 2832618.1 - MES 4.6 support for IBM AIX platform.</p> <p>For patch availability, see section 2.2 Post Release Patches</p>

	12.1.0.2 Patch 34205981 , or Quarterly Full Stack download for SuperCluster (Q3.2022) Patch 34206024 for Solaris SPARC 64-Bit		
Oracle Database Server home	Oracle JavaVM Component Database PSU 12.1.0.2.220719 Patch 34086863 for UNIX, or Oracle JavaVM Component Microsoft Windows Bundle Patch 12.1.0.2.220719 Patch 34185253	CVE-2022-21565	OJVM PSU Patches are not RAC Rolling installable. However, NOTE 2217053.1 defines a few specific situations where the OJVM PSU patchset can be postinstalled into each database while the database remains in unrestricted "startup" mode. Refer to the NOTE for more details. All OJVM PSU since 12.1.0.2.161018 includes Generic JDBC Patch 23727148 See Note 1929745.1 , Oracle Recommended Patches -- Oracle JavaVM Component Database PSU (OJVM PSU) Patches For patch availability, see section 2.2 Post Release Patches
Oracle Database Server, Gateway and Client Home	JDK7u351 Patch 34113570	CVE-2022-34169, CVE-2022-21541, CVE-2022-21540	See Note 2584628.1 , "JDK and PERL Patches for Oracle Database Home and Grid Home" for information on availability and prior patches. JDK patches for 32 bit clients would be build on demand basis.
Oracle Database Server home	Perl Patch 33912892	Released April 2022	See Note 2584628.1 , "JDK and PERL Patches for Oracle Database Home and Grid Home" for information on availability and prior patches.
Oracle Database Server home	Oracle JavaVM Component Database PSU - Generic JDBC 12.1.0.2.160719 Patch 23727148	Released July 2016	
Oracle Database Client, Gateway, and Global Data Services Home	Database PSU 12.1.0.2.220719 Patch 34057742 for UNIX, or Microsoft Windows 32-Bit and x86-64 BP 12.1.0.2.220719 Patch 33883271	CVE-2020-26185, CVE-2020-26184	The Instant Client installation is not the same as the client-only Installation. For additional information about Instant Client installations, see Oracle Call Interface Programmer's Guide .

3.1.8 Oracle Database Mobile/Lite Server

Error Correction Information for Oracle Database Mobile Server

Patch Information	12.1 (Mobile Server)	Comments
Final CPU	April 2023	

Patch Availability for Oracle Database Mobile Server 12.1.x

Product Home	Patch	Advisory Number	Comments
12.1	12.1.0.0 BP Patch 21974980	Released October 2015	

3.1.9 Oracle GoldenGate**Error Correction information for Oracle GoldenGate**

Component	21.3.0.0.0	19.1	12.2.0.2	Comments
Final CPU	April 2024	July 2026	October 2023	

Patch Availability for Oracle GoldenGate

Product Home	Patch	Advisory Number	Comments
21.3.0.0.0	Oracle GoldenGate 21.7.0.0.0 for Oracle Patch 34315139 or later Oracle GoldenGate 21.7.0.0.0 Microservices for Oracle Patch 34315141 or later	CVE-2018-25032, CVE-2022-21551, CVE-2021-3749	Refer to Note 1645495.1 for the latest release and additional platforms. For patch availability, see section 2.2 Post Release Patches
19.1	Oracle GoldenGate 19.1.0.0.220719 for Oracle 11g Patch 34377350 or later Oracle GoldenGate 19.1.0.0.220719 for Oracle 12c Patch 34377368 or later Oracle GoldenGate 19.1.0.0.220719 for Oracle 18c Patch 34377377 or later Oracle GoldenGate 19.1.0.0.220719 for Oracle 19c Patch 34377379 or later	CVE-2018-25032, CVE-2022-21551	Refer to Note 1645495.1 for the latest release and additional platforms. For patch availability, see section 2.2 Post Release Patches
12.3.0.1	Oracle GoldenGate 12.3.0.1.220228 FOR Oracle 11g Patch 33907910 Oracle GoldenGate 12.3.0.1.220228 Microservices for Oracle 11g Patch 33907929 Oracle GoldenGate 12.3.0.1.220228 FOR Oracle 12c Patch 33907922 Oracle GoldenGate 12.3.0.1.220228 Microservices for Oracle 12c Patch 33907931	Released April 2022	Refer to Note 1645495.1 for the latest release and additional platforms
12.2.0.2	On-Request	Released October 2021	Refer to Note 1645495.1 for the latest release and additional platforms.

3.1.10 Oracle GoldenGate for Big Data (Formerly known as Oracle GoldenGate Application Adapters)**Error Correction information for Oracle GoldenGate for Big Data**

Component	21.3.0.0.0	19.1.0.0.x	Comments
Final CPU	-	July 2026	

Patch Availability for Oracle GoldenGate for Big Data

Product Home	Patch	Advisory Number	Comments
21.3.0.0.0	Oracle GoldenGate for Big Data 21.5.0.0.0 Microservices Patch 33846655	Released April 2022	
	Oracle GoldenGate for Big Data 21.5.0.0.0 Patch 33900667	Released April 2022	
19.1.0.0.0	Oracle GoldenGate for Big Data 19.1.0.0.13 Patch 33735336	Released April 2022	
12.3.0.1.0	Oracle GoldenGate for Big Data 12.3.2.1.12 Patch 34023425	Released April 2022	

3.1.11 Oracle GoldenGate Monitor (aka Management Pack for Oracle GoldenGate)

Error Correction information for Oracle GoldenGate Monitor (aka Management Pack for Oracle GoldenGate)

Patch Information	12.2.1	12.1.3.x	Comments
Final CPU	July 2025	July 2022	

Patch Availability for Management Pack For Oracle GoldenGate

Product Home	Patch	Advisory Number	Comments
12.2.1.2.0	Oracle GoldenGate Monitor 12.2.1.2.200930 (Server+Agent) Patch 31748559	Released October 2020	
12.1.3	Monitor Server 12.1.3.0.160628 Patch 23340597 Monitor Agent 12.1.3.0.160628 Patch 23333295	Released June 2016	-

3.1.12 Oracle GoldenGate Veridata

Error Correction information for Oracle GoldenGate Veridata

Component	12.2.1	12.1.3	Comments
Final CPU	July 2025	July 2022	

Patch Availability for Oracle GoldenGate Veridata

Product Home	Patch	Advisory Number	Comments
12.2.1	OGG Veridata Bundle Patch 12.2.1.4.200714 (PS4 BP2) (Server+Agent) Patch 31044508	Released July 2020	

Product Home	Patch	Advisory Number	Comments
12.1.3	ORACLE GOLDENGATE VERIDATA V12.1.3.0.180415 SERVER Patch 26424104	Released April, 2018	

3.1.13 Oracle NoSQL Database

Minimum Product Requirements for Oracle NoSQL Database

Critical Patch Update security vulnerabilities are fixed in the listed releases. The Oracle NoSQL Database downloads and installation instructions can be found at <https://www.oracle.com/database/technologies/nosql-database-server-downloads.html>

Product	Release	Advisory Number	Comments
Oracle NoSQL Database	21.1.12	CVE-2021-43797	

3.1.14 Oracle Secure Backup

Error Correction information for Oracle Secure Backup

Patch Information	18.1	Comments
Final CPU	January 2024	

Minimum Product Requirements for Oracle Secure Backup

Critical Patch Update security vulnerabilities are fixed in the listed releases. The Oracle Secure Backup downloads and installation instructions can be found at <http://www.oracle.com/technetwork/database/database-technologies/secure-backup/overview/index.html>

Product	Release	Advisory Number	Comments
Oracle Secure Backup	18.1.0.2	Released April 2022	

3.1.15 Oracle Spatial Studio

Minimum Product Requirements for Oracle Spatial Studio

Critical Patch Update security vulnerabilities are fixed in the listed releases. The Oracle Spatial Studio downloads and installation instructions can be found at <https://www.oracle.com/database/technologies/spatial-studio/oracle-spatial-studio-downloads.html>

Product	Release	Advisory Number	Comments
Oracle Spatial Studio	22.1.2	CVE-2020-36518	

3.1.16 Oracle SQL Developer

Minimum Product Requirements for Oracle SQL Developer

Critical Patch Update security vulnerabilities are fixed in the listed releases. The Oracle SQL Developer downloads and installation instructions can be found at <https://www.oracle.com/tools/downloads/sqldev-downloads.html>

Product	Release	Advisory Number	Comments
Oracle SQL Developer	22.2.0.173.2018	CVE-2021-31812, CVE-2021-31811	Announced as part of Log4j security alert

(<https://www.oracle.com/security-alerts/alert-cve-2021-44228.html>)

Refer to [Note 2828123.1](#) for more details on SQL Developer installation

3.1.17 Oracle Stream Analytics

Minimum Product Requirements for Oracle Stream Analytics

Critical Patch Update security vulnerabilities are fixed in the listed releases. The Oracle Stream Analytics downloads and installation instructions can be found at

<https://www.oracle.com/middleware/technologies/stream-analytics/downloads.html>

Product	Patch	Advisory Number	Comments
Oracle Stream Analytics	ORACLE STREAM ANALYTICS 19.1.0.0.7 Patch 34010471	CVE-2021-37714, CVE-2021-34429	

3.1.18 Oracle TimesTen In-Memory Database

Error Correction information for Oracle TimesTen In-Memory Database

Describes Error Correction information for Oracle TimesTen In-Memory Database. The Oracle TimesTen In-Memory Database downloads and installation instructions can be found at

<https://www.oracle.com/in/database/technologies/timesten-downloads.html>

Patch Information	18.1	Comments
Final Patch	April 2026	

Minimum Product Requirements for Oracle TimesTen In-Memory Database

Describes the minimum product requirements for Oracle TimesTen In-Memory Database. The CPU security vulnerabilities are fixed in the listed release and later releases.

Product	Release	Advisory Number	Comments
Oracle TimesTen In-Memory Database	22.1.1.2.0 or later version	CVE-2021-2351, CVE-2022-23806, CVE-2021-41771, CVE-2021-41772, CVE-2022-23772, CVE-2022-23773, CVE-2022-23305, CVE-2021-4104, CVE-2022-23302 and CVE-2022-23307	

3.1.19 Oracle Essbase

Error Correction information for Oracle Essbase

Describes Error Correction information for Oracle Essbase.

Patch Information	21.c	Comments
Final Patch	July 2025	

Minimum Product Requirements for Oracle Essbase

Describes the minimum product requirements for Oracle Essbase. The CPU security vulnerabilities are fixed in the listed release and later releases.

Product Home	Patch	Advisory Number	Comments
21.x	21.3.0.0.0 ORACLE ESSBASE RELEASE UPDATE Patch 32646479	CVE-2022-21508	

3.2 Oracle Sun Middleware

This section contains the following:

- [Section 3.2.1 "Directory Server Enterprise Edition"](#)

3.2.1 Directory Server Enterprise Edition

Error Correction information for Directory Server Enterprise Edition

Patch Information	11.1.1.7.0	Comments
Final CPU (Premier Support)	October 2019	
Final CPU (Extended Support)	October 2022	

Patch Availability for Directory Server Enterprise Edition

Product Home	Patch	Advisory Number	Comments
11.1.1.7.0	ODSEE BP 11.1.1.7.190716 Patch 29893742	Released July 2019	CVE-2018-18508 is not applicable to Windows Platform. Refer to 2.2 Post Release Patches for Windows Patch.

3.3 Tools

This section contains the following:

- [Section 3.3.1 "Oracle OPatch"](#)

3.3.1 Oracle OPatch

Minimum Product Requirements for Oracle OPatch

The CPU security vulnerabilities are fixed in the listed release and later releases. The Oracle OPatch downloads can be found at [Patch 6880880](#).

Component	Release	Advisory Number	Comments
Oracle OPatch	11.2.0.3.35 or Later Version, 12.2.0.1.31 or Later Version	CVE-2022-23437, CVE-2020-36518	Download the latest versions available to install Database Patches

4 Final CPU History

Final CPU History

The Final CPU is the last quarter that a product is supported in the CPU program as per the Premier Support and Extended Support policies. For more information, see My Oracle Support [Note 209768.1](#), *Database, FMW, EM Grid Control, and OCS Software Error Correction Support Policy*.

Release	Final CPUs	Comments
January 2022		

5 Sources of Additional Information

The following documents provide additional information about Critical Patch Updates:

- My Oracle Support [Note 888.1](#), *Primary Note for Database Proactive Patch Program*
- My Oracle Support [Note 209768.1](#), *Database, FMW, Enterprise Manager, TimesTen In-Memory Database, and OCS Software Error Correction Support Policy*

6 Modification History

Modification History

Date	Modification
July 19, 2022	Released Updated patch availability in section 2.2 Updated 'Comments' for patch 34377350 in section 3.1.9 Updated 'Release' in section 3.3.1
July 20, 2022	Updated patch availability in section 2.2
July 21, 2022	Updated patch availability in section 2.2
July 22, 2022	Updated patch availability in section 2.2
July 25, 2022	Updated patch availability in section 2.2 Updated 'Advisory Number' in first and second row of section 3.1.7.3
July 26, 2022	Updated patch availability in section 2.2 Updated 'Advisory Number' in first and second row of section 3.1.7.4 Updated 'Advisory Number' in first row of section 3.1.7.2
July 27, 2022	Updated patch availability in section 2.2
July 28, 2022	Updated patch availability in section 2.2
August 05, 2022	Updated patch availability in section 2.2

7 Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> or visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> if you are hearing impaired.

Critical Patch Update Availability Document July 2022

Copyright © 2006, 2022, Oracle and/or its affiliates.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, Report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

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.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Didn't find what you are looking for?