Critical Patch Update (CPU) Program Apr 2022 Patch Availability Document (DB-only) (Doc ID 2844795.1)

APPLIES TO:

Oracle Database Backup Service - Version N/A and later
Oracle Database Exadata Express Cloud Service - Version N/A and later
Oracle Database - Standard Edition - Version 12.1.0.2 and later
Oracle Database Cloud Schema Service - Version N/A and later
Oracle Database Cloud Service - Version N/A and later
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 April 19, 2022.

SCOPE

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

DETAILS

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

My Oracle Support Note 2844795.1

Released April 19, 2022

This document contains the following sections:

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 April 2022, available at:

Oracle Technical Network Advisory

This document lists the Oracle Database CPU program cumulative patches for product releases under error correction. The April 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:

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 April 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 April 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 April 2022

This section describes important changes in April 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 Apr 2022

- none

Final CPUs scheduled for Jul 2022

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

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.

Patch	Patch Number	Platform	Availability
Database Release Update 21.6.0.0.220419	Patch 33843745	HP-UX Itanium	Available

GI Release Update 21.6.0.0.220419	Patch 33859395	HP-UX Itanium	Available
DB RU 19.15.0.0.220419 (& associated COMBO)	Patch 33806152 (& Patch 33859194)	All except Linux x86-64	Available
GI RU 19.15.0.0.220419 (& associated COMBO)	Patch 33803476 (& Patch 33859214)	All except Linux x86-64	Available
Database RUR 19.14.1.0.220419	Patch 33806138	Linux x86-64	Available
		Solaris Sparc64, Solaris x86-64, zLinux, HP-UX Itanium, AIX	Available
GI Release Update Revision 19.14.1.0.220419	Patch 33785101	Linux x86-64	Available
		Solaris Sparc64, Solaris x86-64, zLinux, HP-UX Itanium, AIX	Available
Database RUR 19.13.2.0.220419	Patch 33783771	All	Available
GI Release Update Revision 19.13.2.0.220419	Patch 33881789	All	Available
DBBP 12.1.0.2.220419 (& associated COMBO)	Patch 33880550 (& Patch 33859530)	AIX	Available
		HP-UX Itanium	Available
DB PSU 12.1.0.2.220419 (& associated COMBO)	Patch 33711081 (& Patch 33859494)	HP-UX Itanium	Available
GI PSU 12.1.0.2.220419 (& associated COMBO)	Patch 33829718 (& Patch 33859511)	HP-UX Itanium	Available
OJVM Release Update 19.15.0.0.220419	Patch 33808367	MS-Windows	Available
OJVM Component Database PSU 12.1.0.2.220419	Patch 33808385	HP-UX Itanium	Available
Microsoft Windows BP 21.6.0.0.220419	Patch 33829143	MS-Windows	Available
Microsoft Windows BP 19.15.0.0.220419	Patch 33829175	MS-Windows	Available
QFSDP for Exadata (Apr2022) 21.6	Patch 33881715	All	Available
QFSDP for Exadata (Apr2022) 19.15	Patch 33881712	All	Available
QFSDP for Exadata (Apr2022) 12.1.0.2	Patch 33881695	All	Available
QFSDP for SuperCluster (Q2.2022)	Patch 33881722	All	Available

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 2844807.1
- 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:

3.1 Oracle Database

This section contains the following:

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	21.3	CVE-2021-29425	

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	21.1.0 Bundle Patch Patch 32598392 or later	CVE-2021-41165, CVE-2021-41164	

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	Released April 2022	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	CVE-2021-23017, CVE-2020-5245, CVE-2020-8174, CVE-2020-24750, CVE-2020-28052, CVE-2019-12399, CVE-2020-17527, CVE-2020-11612, CVE-2019-13565, CVE-2020-8203, CVE-2019-10086, CVE-2020-11022, CVE-2021-29425, CVE-2020-27218, CVE-2017-14159, CVE-2017-17740, CVE-2017-9287, CVE-2019-13057, CVE-2020-12243, CVE-2020-15719, CVE-2020-13935, CVE-2020-24616, CVE-2020-25649, CVE-2020-36189, CVE-2020-10531, CVE-2020-11080, CVE-2020-8172, CVE-2020-8277	
Oracle Blockchain Platform - Enterprise Edition	Hotfix for OBPEE 21.1.2 Patch 33795456	CVE-2021-2351	

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

Component	Release	Advisory Number	Comments
Oracle Graph Server and Client	21.4.2.0.0	Released January 2022	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 21.4.2 (released December 2021) should replace all installations of graph feature of Oracle Big Data Spatial and Graph.	Released January 2022	Steps to replace BDSG 3.0 and all prior installations with Oracle Graph Server and Client 21.4.2: (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 21.4.2 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:

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 21.6.0.0.220419 Patch 33843745 for UNIX, or GI Release Update 21.6.0.0.220419 Patch 33859395, or Microsoft Windows 32-Bit and x86-64 BP 21.6.0.0.220419 Patch 33829143 or later, or Quarterly Full Stack download for Exadata (Apr2022) 21.6 Patch 33881715 for Linux x86-64, or	CVE-2021-22569, CVE-2021-2464, CVE-2021-30129, CVE-2019-12402, CVE-2021-42340	**21c does not have COMBO nor OJVM patches. Instead, the OJVM fixes are contained within the DB RU and the GU 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	JDK8u331 Patch 33810177	CVE-2022-21476, CVE-2022-21426, CVE-2022-21496, CVE-2022-21434, CVE-2022-21443	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	CVE-2022-23990, CVE-2022-23852	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 21.6.0.0.220419 Patch 33843745 for UNIX	CVE-2022-21411 (Gateway Home Only)	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 Server home	Combo OJVM Release Update 19.15.0.0.220419 and Database Release Update 19.15.0.0.220419 Patch 33859194 for UNIX, or	CVE-2021-22569, CVE-2022-21410, CVE-2021-2464, CVE-2022-21498, CVE-2021-42340	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

	Combo OJVM Release Update 19.15.0.0.220419 and GI Release Update 19.15.0.0.220419 Patch 33859214, or Quarterly Full Stack download for Exadata (Apr2022) 19.15 Patch 33881712 for Linux x86-64		
Oracle Database Server home	Database Release Update 19.15.0.0.220419 Patch 33806152 for UNIX, or GI Release Update 19.15.0.0.220419 Patch 33803476, or Microsoft Windows 32-Bit and x86-64 BP 19.15.0.0.220419 Patch 33829175 or later, or Database Release Update Revision 19.14.1.0.220419 Patch 33806138 for UNIX, or GI Release Update Revision 19.14.1.0.220419 Patch 33785101, or Database Release Update Revision 19.13.2.0.220419 Patch 33783771 for UNIX, or GI Release Update Revision 19.13.2.0.220419 Patch 33881789, or Quarterly Full Stack download for Exadata (Apr2022) 19.15 Patch 33881712 for Linux x86-64, or Quarterly Full Stack download for SuperCluster (Q2.2022) Patch 33881722 for Solaris SPARC 64-Bit	CVE-2021-22569, CVE-2022-21410, CVE-2021-2464	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. 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. 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 For patch availability, see section 2.2 Post Release Patches
Oracle		CVE-2022-	

Database Server home	OJVM Release Update 19.15.0.0.220419 Patch 33808367 for all platforms	21498	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	JDK8u331Patch 33810130	CVE-2022-21476, CVE-2022-21426, CVE-2022-21496, CVE-2022-21434, CVE-2022-21443	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	CVE-2022-23990, CVE-2022-23852	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 19.15.0.0.220419 Patch 33806152 for UNIX, or Database Release Update Revision 19.14.1.0.220419 Patch 33806138 for UNIX, or Database Release Update Revision 19.13.2.0.220419 Patch 33783771 for UNIX, or Microsoft Windows 32-Bit and x86-64 BP 19.15.0.0.220419 Patch 33829175	CVE-2022-21411 (Gateway Home Only)	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		CVE-2021-2464,	

Database Server home	Combo OJVM PSU 12.1.0.2.220419 and Database Proactive BP 12.1.0.2.220419 Patch 33859530 for UNIX, or Combo OJVM PSU 12.1.0.2.220419 and Database PSU 12.1.0.2.220419 Patch 33859494 for UNIX, or Combo OJVM PSU 12.1.0.2.220419 and GI PSU 12.1.0.2.220419 Patch 33859511, or Quarterly Full Stack download for Exadata (Apr2022) 12.1.0.2 Patch 33881695, or Quarterly Full Stack download for SuperCluster (Q2.2022) Patch 33881722 for Solaris SPARC 64-Bit	CVE-2022-21498	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. Combos are for environments that take a single downtime to apply all patches 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 home	Database Proactive Bundle Patch 12.1.0.2.220419 Patch 33880550, or Database PSU 12.1.0.2.220419 Patch 33711081 for UNIX, or GI PSU 12.1.0.2.220419 Patch 33829718, or Microsoft Windows 32-Bit and x86-64 BP 12.1.0.2.220419 Patch 33777450 or later, or Quarterly Full Stack download for Exadata (Apr2022) 12.1.0.2 Patch 33881695, or Quarterly Full Stack download for SuperCluster (Q2.2022) Patch 33881722 for Solaris SPARC 64-Bit	CVE-2021-2464	For JDK fixes a separate patch is available (see below) and needs to be installed in addition to the Database and GI patches. 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 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. For patch availability, see section 2.2 Post Release Patches

Oracle Database Server home	Oracle JavaVM Component Database PSU 12.1.0.2.220419 Patch 33808385 for UNIX, or Oracle JavaVM Component Microsoft Windows Bundle Patch 12.1.0.2.220419 Patch 33881387	CVE-2022-21498	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	JDK7u341Patch 33810237	CVE-2022-21476, CVE-2022-21426, CVE-2022-21496, CVE-2022-21434, CVE-2022-21443	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	CVE-2022-23990, CVE-2022-23852	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 12.1.0.2.220419 Patch 33711081 for UNIX, or Microsoft Windows 32-Bit and x86-64 BP 12.1.0.2.220419 Patch 33777450	CVE-2022-21411 (Gateway Home Only)	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 21.6.0.0.0 for Oracle Patch 34009130 or later Oracle GoldenGate 21.6.0.0.0 Microservices for Oracle Patch 34009136 or later	CVE-2022-21442	Refer to Note 1645495.1 for the latest release and additional platforms.
19.1	Oracle GoldenGate 19.1.0.0.220419 for Oracle 11g Patch 34008737 or later Oracle GoldenGate 19.1.0.0.220419 for Oracle 12c Patch 34008747 or later Oracle GoldenGate 19.1.0.0.220419 for Oracle 18c Patch 34008757 or later Oracle GoldenGate 19.1.0.0.220419 for Oracle 19c Patch 34008763 or later	CVE-2022-21442	Refer to Note 1645495.1 for the latest release and additional platforms.
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	CVE-2019-12086, CVE-2019-14862	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

Product Home	Patch	Advisory Number	Comments
21.3.0.0.0	Oracle GoldenGate for Big Data 21.5.0.0.0 Microservices Patch 33846655 Oracle GoldenGate for Big Data 21.5.0.0.0 Patch 33900667	CVE-2021-26291, CVE-2021-2351, CVE-2022-23305, CVE-2019-17571, CVE-2021-4104, CVE-2022-23302 CVE-2021-44228	
19.1.0.0.0	Oracle GoldenGate for Big Data 19.1.0.0.13 Patch 33735336	CVE-2021-2351, CVE-2022-23305, CVE-2019-17571, CVE-2021-4104, CVE-2022-23302	
12.3.0.1.0	Oracle GoldenGate for Big Data 12.3.2.1.12 Patch 34023425	CVE-2021-29425	

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	
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-2021-37137, CVE-2021-21290, CVE-2021-21295, CVE-2021-21409, CVE-2021-30129, CVE-2021-37136	

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	CVE-2021-44790, CVE-2021-32785, CVE-2021-32786, CVE-2021-32791, CVE-2021-32792, CVE-2021-44224, CVE-2021-21703	

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	21.2.1	Released January 2022	

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	21.4.2.018.1706	Released January 2022 - CVE-2021-44832, CVE-2020-13956	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	19.1.0.0.6 MLR Patch 33750861	Released January 2022	

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	22.1.1.1.0 or later version	Released January 2022	

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	Released January 2022	

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	11.2.0.3.33, 12.2.0.1.29	Released January 2022	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	Oracle GoldenGate for Big Data 12.3.2.1.11	

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
April 19, 2022	Released Updated Advisory Number in section 3.1.16
April 20, 2022	Updated patch availability in section 2.2
April 22, 2022	Updated patch availability in section 2.2 Updated Advisory Number for 12.3.0.1 in section 3.1.9 Updated Product Home for Patch 34023425 in section 3.1.10
April 27, 2022	Updated patch availability in section 2.2
May 02, 2022	Updated patch availability in section 2.2
May 09, 2022	Updated patch availability in section 2.2
May 11, 2022	Updated the 'Advisory Number' column for Patch 33810177 in section 3.1.7.2 Updated the 'Advisory Number' column for Patch 33810130 in section 3.1.7.3 Updated the 'Advisory Number' column for Patch 33810237 in section 3.1.7.4
May 16, 2022	Updated patch availability in section 2.2
May 18, 2022	Updated patch availability in section 2.2
May 24, 2022	Updated patch availability in section 2.2
June 02, 2022	Updated patch availability in section 2.2
June 06, 2022	Updated patch availability in section 2.2
June 07, 2022	Updated patch availability in section 2.2 Added comment for Note 2584628.1 to sections 3.1.7.2, 3.1.7.3, and 3.1.7.4

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 April 2022

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.