Today. Tomorrow. Together.

Oracle Security and Patching

September 17th 2024

itm8

Lets start out with a four questions ?

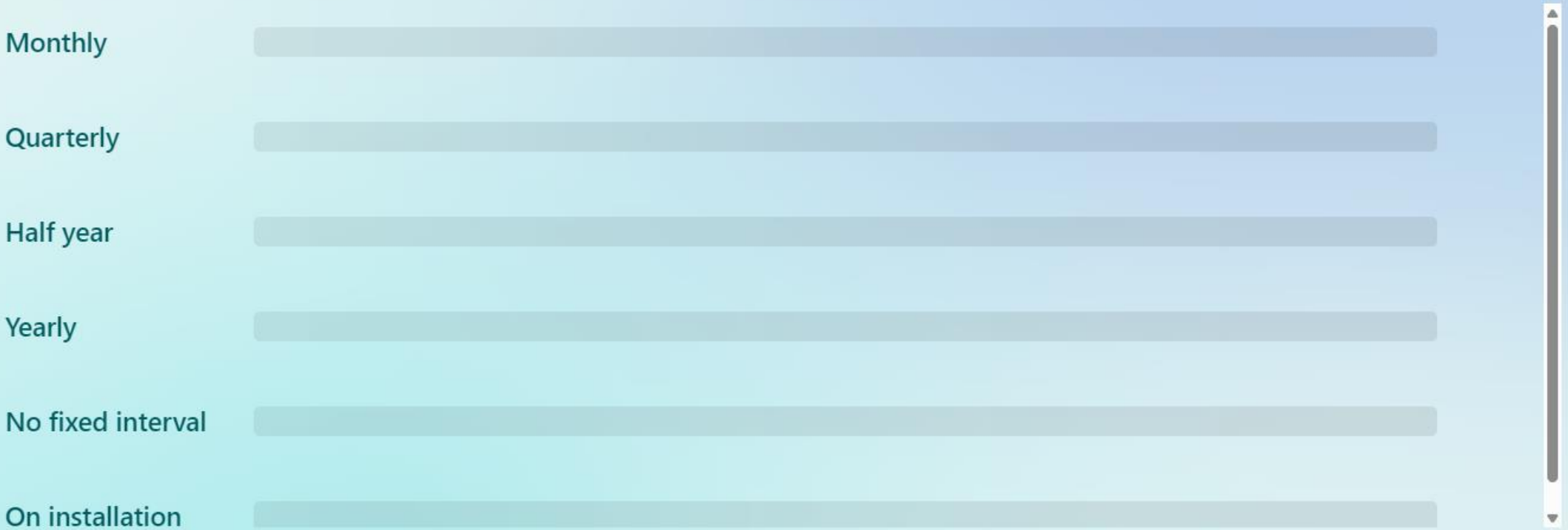
0 response submitted

What platform(s) are you running Oracle on?

- Oracle Linux
- Other Linux distribution
- Solaris
- AIX
- Microsoft Windows
- Other

0 response submitted

How often do you patch your OS?



Treemap | Bar

1 of 1

0 response submitted

What Database versions are you running in production

11 or older

12.1.0.X

12.2.0.1

18

19

21

23

0 response submitted

How often do you patch your Oracle DB SW?

Quarterly

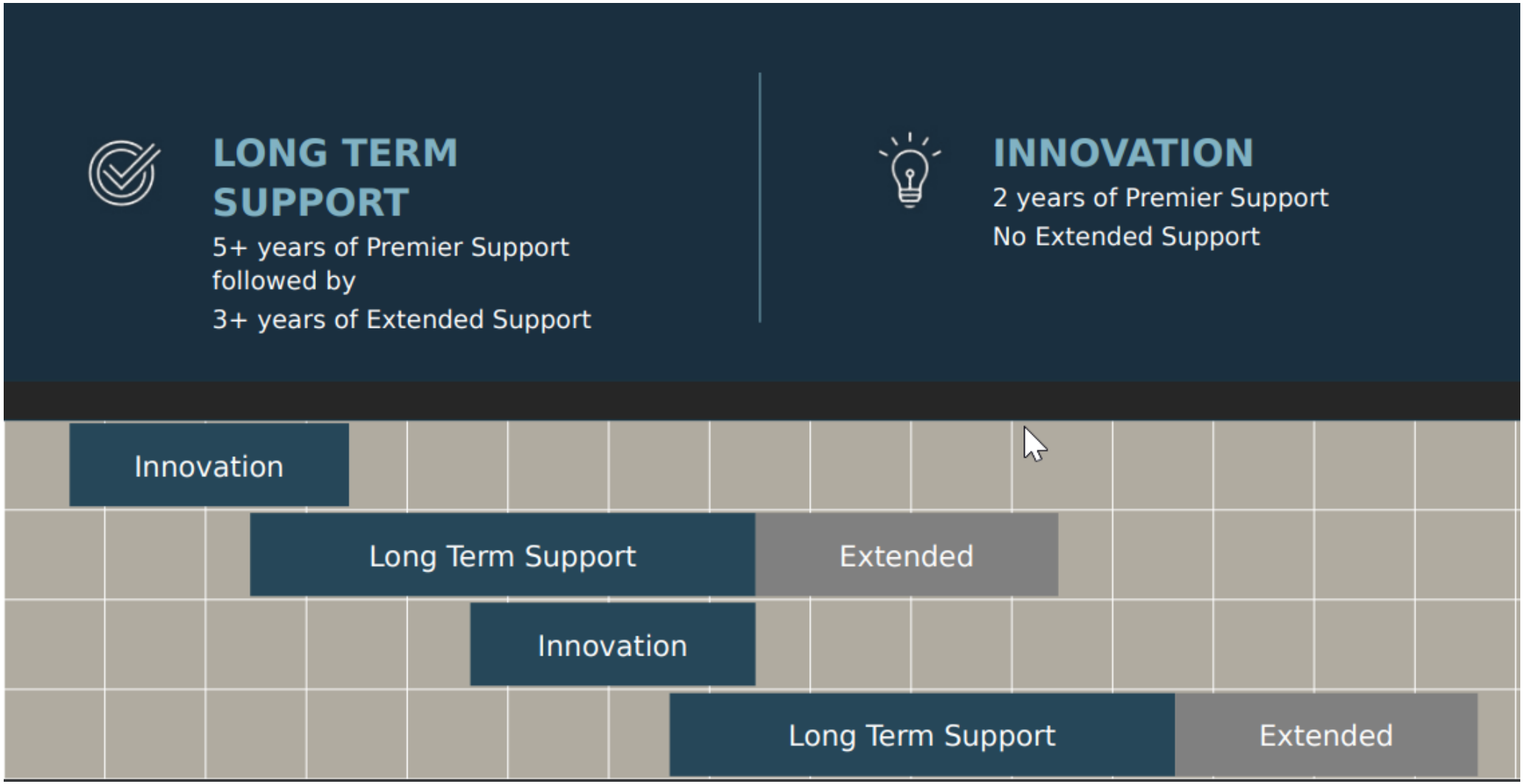
Half year

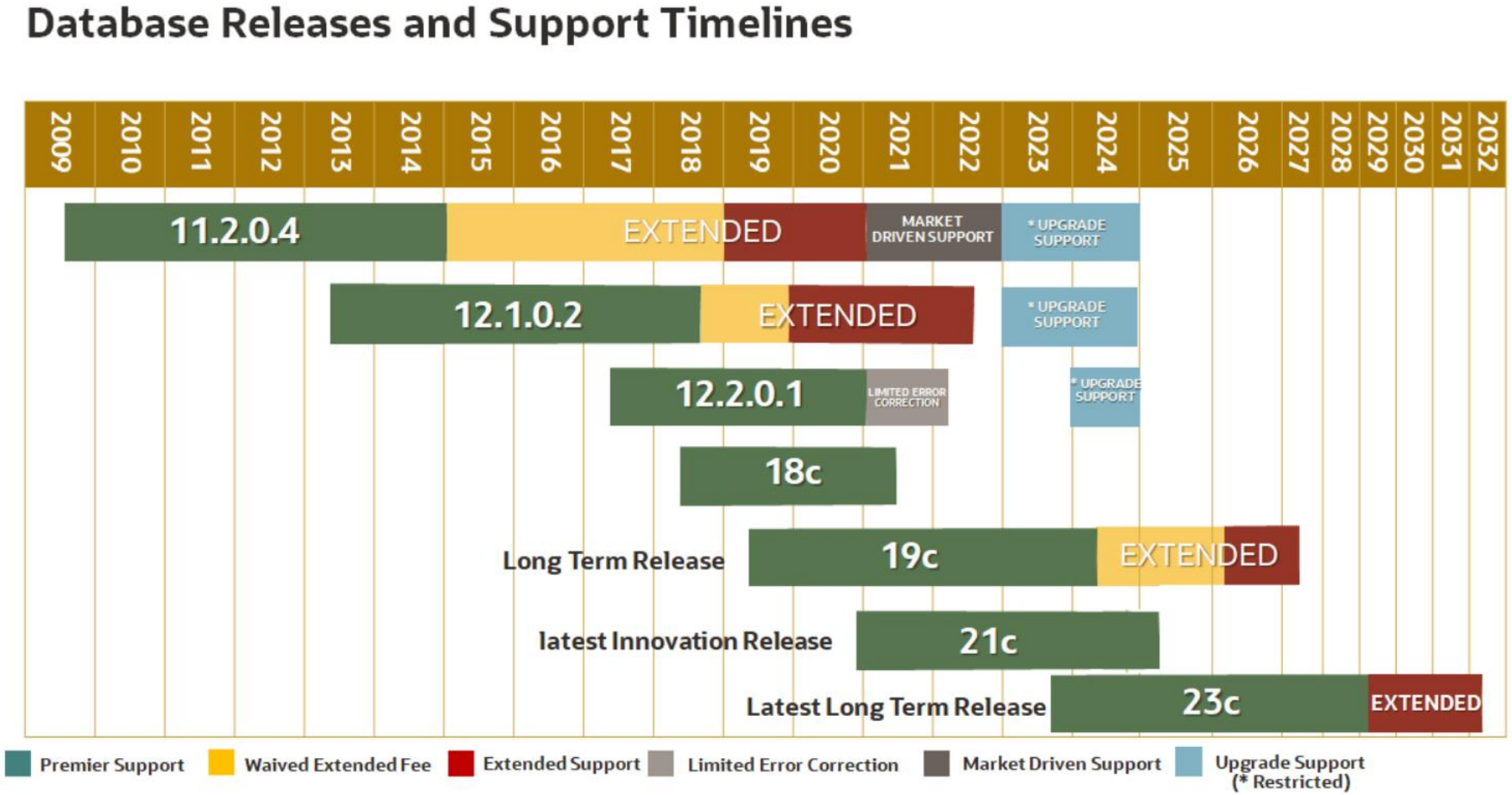
Yearly

No specific interval

On installation

Long term vs innovation releases




Database Releases and Support Timelines
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2030
2031
2032
11.2.0.4
EXTENDED
MARKET DRIVEN SUPPORT
* UPGRADE SUPPORT
12.1.0.2
EXTENDED
* UPGRADE SUPPORT
12.2.0.1
LIMITED ERROR CORRECTION
* UPGRADE SUPPORT
18c
Long Term Release
19c
EXTENDED
latest Innovation Release
21c
Latest Long Term Release
23c
EXTENDED
Premier Support
Waived Extended Fee
Extended Support
Limited Error Correction
Market Driven Support
Upgrade Support (* Restricted)

itm8

RELEASE SCHEDULE OF CURRENT DATABASE RELEASES (DOC ID 742060.1)

Table 1 - Patching End Dates for Roadmap

Release	Patching End Date	Notes and Exceptions
23c **Long Term Release**	**April 2032**	• Initially available on OCI Base Database Service. Will become available on other platforms (cloud and on-premises) starting 1H CY2024.
21c **Innovation Release**	**April 30, 2025**	• Error Correction / Patching is available until **April 30, 2025** • 21c is not eligible for Extended Support (ES) • Only quarterly Release Updates (RUs) are provided for 21c. • 21c is not available with Exadata Database Service
19c **Long Term Release**	UPD **April 30, 2026 with no ES/ULA** **April 30, 2027 with ES/ULA**	• Premier Support (PS) ends April 30, 2024, two years of waived Extended Support (ES) fees will be in effect from May 1, 2024 until April 30, 2026. Fees will be required beginning May 01, 2026 through April 30, 2027 • Error Correction / Patching is available through April 30, 2027 with paid ES. Without paid ES, patching is only available until April 30, 2026 • Beginning with the October 2022 patching cycle, 19c RURs will no longer be provided for 19.17.0 and above. No additional RURs will be delivered on any platform after the delivery of Oracle Database 19c RUR 19.16.2 in January 2023. (Refer to Sunsetting of 19c RURs and FAQ (Doc ID 2898381.1) for further details.) To provide customers more frequent access to recommended and well-tested collections of patches, Oracle is pleased to introduce Monthly Recommended Patches (MRPs) starting Nov 2022. MRPs are supported only on the Linux x86-64 platform. (Refer to Introducing Monthly Recommended Patches (MRPs) and FAQ (Doc ID 2898740.1) for further details.) •

Oracle Critical Patch Update [CPU]

Are released each Quarter of the year in:

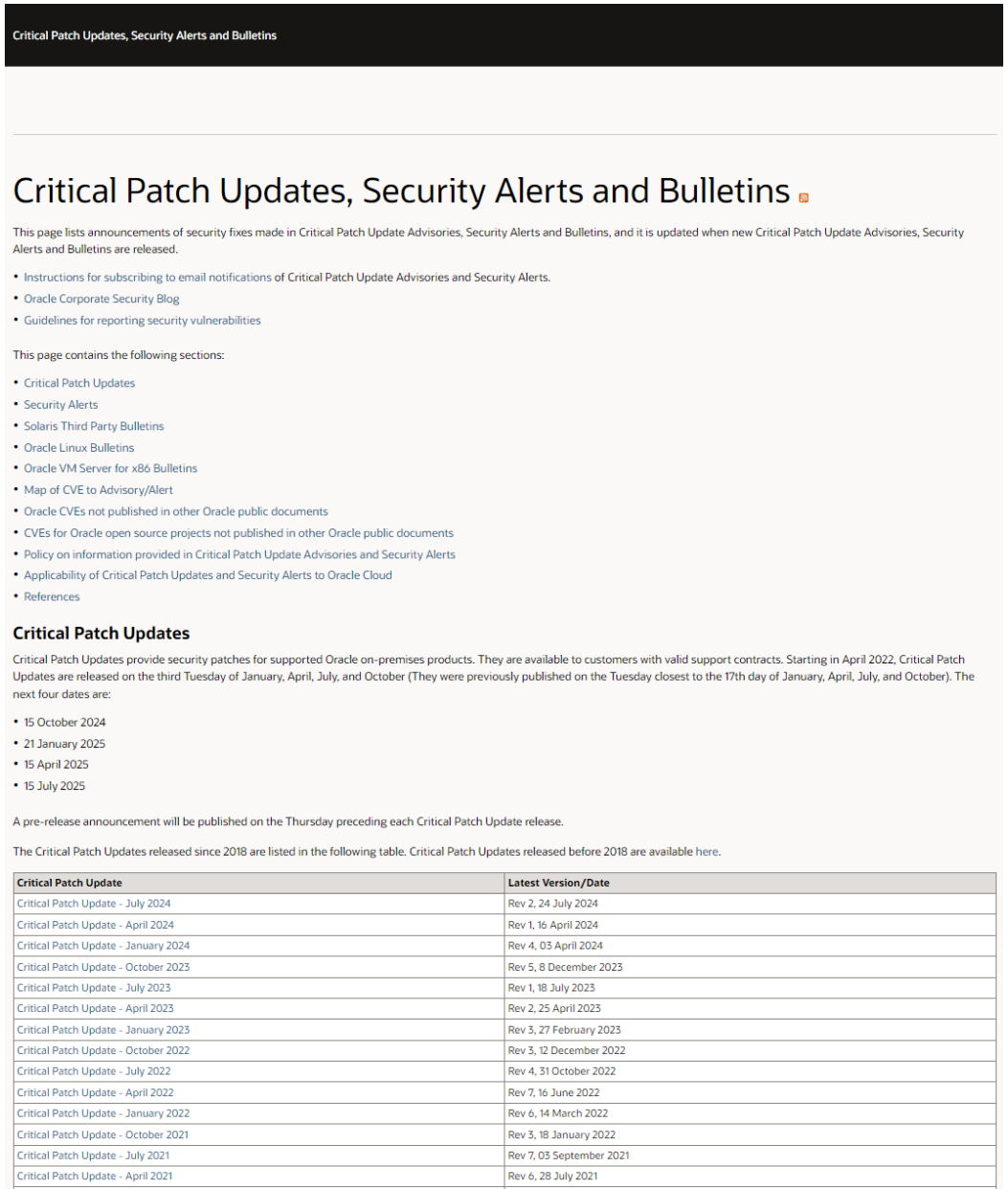
- October
- January
- April
- July

For the current Database versions we are now on patch:

- 19.24.0.0.240716
- 21.15.0.0.240716

Critical Patch Updates

https://www.oracle.com/security-alerts/



Critical Patch Updates, Security Alerts and Bulletins

Critical Patch Updates, Security Alerts and Bulletins

This page lists announcements of security fixes made in Critical Patch Update Advisories, Security Alerts and Bulletins, and it is updated when new Critical Patch Update Advisories, Security Alerts and Bulletins are released.

- Instructions for subscribing to email notifications of Critical Patch Update Advisories and Security Alerts.
- Oracle Corporate Security Blog
- Guidelines for reporting security vulnerabilities

This page contains the following sections:

- Critical Patch Updates
- Security Alerts
- Solaris Third Party Bulletins
- Oracle Linux Bulletins
- Oracle VM Server for x86 Bulletins
- Map of CVE to Advisory/Alert
- Oracle CVEs not published in other Oracle public documents
- CVEs for Oracle open source projects not published in other Oracle public documents
- Policy on information provided in Critical Patch Update Advisories and Security Alerts
- Applicability of Critical Patch Updates and Security Alerts to Oracle Cloud
- References

Critical Patch Updates

Critical Patch Updates provide security patches for supported Oracle on-premises products. They are available to customers with valid support contracts. Starting in April 2022, Critical Patch Updates are released on the third Tuesday of January, April, July, and October (They were previously published on the Tuesday closest to the 17th day of January, April, July, and October). The next four dates are:

- 15 October 2024
- 21 January 2025
- 15 April 2025
- 15 July 2025

A pre-release announcement will be published on the Thursday preceding each Critical Patch Update release.

The Critical Patch Updates released since 2018 are listed in the following table. Critical Patch Updates released before 2018 are available here.

Critical Patch Update	Latest Version/Date
Critical Patch Update - July 2024	Rev 2, 24 July 2024
Critical Patch Update - April 2024	Rev 1, 16 April 2024
Critical Patch Update - January 2024	Rev 4, 03 April 2024
Critical Patch Update - October 2023	Rev 5, 8 December 2023
Critical Patch Update - July 2023	Rev 1, 18 July 2023
Critical Patch Update - April 2023	Rev 2, 25 April 2023
Critical Patch Update - January 2023	Rev 3, 27 February 2023
Critical Patch Update - October 2022	Rev 3, 12 December 2022
Critical Patch Update - July 2022	Rev 4, 31 October 2022
Critical Patch Update - April 2022	Rev 7, 16 June 2022
Critical Patch Update - January 2022	Rev 6, 14 March 2022
Critical Patch Update - October 2021	Rev 3, 18 January 2022
Critical Patch Update - July 2021	Rev 7, 03 September 2021
Critical Patch Update - April 2021	Rev 6, 28 July 2021

itm8

JULY
2024

Oracle Database Products Risk Matrices

This Critical Patch Update contains 15 new security patches for Oracle Database Products divided as follows:

- 8 new security patches for Oracle Database Products
- 1 new security patch for Oracle Application Express
- No new security patches for Oracle Big Data Spatial and Graph, but third party patches are provided
- 2 new security patches for Oracle Essbase
- 1 new security patch for Oracle GoldenGate
- No new security patches for Oracle Graph Server and Client, but third party patches are provided
- 1 new security patch for Oracle NoSQL Database
- 1 new security patch for Oracle REST Data Services
- 1 new security patch for Oracle TimesTen In-Memory Database

Oracle Database Server Risk Matrix

This Critical Patch Update contains 8 new security patches, plus additional third party patches noted below, for Oracle Database Products. 3 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. 1 of these patches is applicable to client-only installations, i.e., installations that do not have the Oracle Database Server installed. The English text form of this Risk Matrix can be found here.

CVE ID	Component	Package and/or Privilege Required	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RISK (see Risk Matrix Definitions)									Supported Versions Affected	Notes
					Base Score	Attack Vector	Attack Complex	Privs Req'd	User Interact	Scope	Confid-entiality	Inte-grity	Avail-ability		
CVE-2022-41881	Fleet Patching and Provisioning (Netty)	None	HTTP	Yes	7.5	Network	Low	None	None	Un-changed	None	None	High	23.4	
CVE-2024-21184	Oracle Database RDBMS Security	Execute on SYS.XS_DIAG	Oracle Net	No	7.2	Network	Low	High	None	Un-changed	High	High	High	19.3-19.23	
CVE-2024-21126	Oracle Database Portable Clusterware	None	DNS	Yes	5.8	Network	Low	None	None	Changed	None	None	Low	19.3-19.23, 21.3-21.14	
CVE-2024-4603	Oracle Database Core (OpenSSL)	None	Multiple	Yes	5.3	Network	Low	None	None	Un-changed	None	None	Low	23.4	
CVE-2024-21098	Multilingual Engine	Authenticated User	Oracle Net	No	4.3	Network	Low	Low	None	Un-changed	None	None	Low	21.3-21.14, 23.4	
CVE-2024-0397	OML4Py (Python)	Authenticated User	HTTPS	No	4.3	Network	Low	Low	None	Un-changed	None	None	Low	21.3-21.14, 23.4	
CVE-2024-21174	Java VM	Create Session, Create Procedure	Oracle Net	No	3.1	Network	High	Low	None	Un-changed	None	None	Low	19.3-19.23, 21.3-21.14, 23.4	
CVE-2024-21123	Oracle Database Core	SYSDBA	Oracle Net	No	2.3	Local	Low	High	None	Un-changed	None	Low	None	19.3-19.23	

Additional CVEs addressed are:

- The patch for CVE-2022-41881 also addresses CVE-2022-41915.
- The patch for CVE-2024-4603 also addresses CVE-2024-2511 and CVE-2024-4741.

Additional patches included in this Critical Patch Update for the following non-exploitable CVEs for this Oracle product family:

- Oracle Database Core (Intel(R) C++ Compiler Classic): CVE-2022-25987 [VEX Justification: vulnerable_code_not_present].
- Oracle Database Core (Perl): CVE-2023-52425 and CVE-2023-52426 [VEX Justification: vulnerable_code_cannot_be_controlled_by_adversary].
- Oracle Database Core (Zlib): CVE-2023-45853 and CVE-2022-37434 [VEX Justification: vulnerable_code_not_present].
- Oracle Database Workload Manager (Jetty): CVE-2024-22201 [VEX Justification: vulnerable_code_not_in_execute_path].
- Oracle Spatial and Graph (curl): CVE-2024-0853 [VEX Justification: vulnerable_code_cannot_be_controlled_by_adversary].

Oracle Database Server Client-Only Installations

- The following Oracle Database Server vulnerability included in this Critical Patch Update affects client-only installations: CVE-2024-4603.

APRIL
2024

Oracle Database Products Risk Matrices

This Critical Patch Update contains 12 new security patches for Oracle Database Products divided as follows:

- 8 new security patches for Oracle Database Products
- 1 new security patch for Oracle Autonomous Health Framework
- 1 new security patch for Oracle Big Data Spatial and Graph
- No new security patches for Oracle Essbase, but third party patches are provided
- 1 new security patch for Oracle Global Lifecycle Management
- 1 new security patch for Oracle GoldenGate
- No new security patches for Oracle TimesTen In-Memory Database, but third party patches are provided

Oracle Database Server Risk Matrix

This Critical Patch Update contains 8 new security patches, plus additional third party patches noted below, for Oracle Database Products. 3 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. None of these patches are applicable to client-only installations, i.e., installations that do not have the Oracle Database Server installed. The English text form of this Risk Matrix can be found here.

CVE ID	Component	Package and/or Privilege Required	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RISK (see Risk Matrix Definitions)									Supported Versions Affected	Notes
					Base Score	Attack Vector	Attack Complex	Privs Req'd	User Interact	Scope	Confid-entiality	Inte-grity	Avail-ability		
CVE-2023-48795	Grid Infrastructure (Apache Mina SSHD)	None	SSH	Yes	5.9	Network	High	None	None	Un-changed	None	High	None	21.3-21.13	
CVE-2023-48795	Oracle SQLcl (Apache Mina SSHD)	None	SSH	Yes	5.9	Network	High	None	None	Un-changed	None	High	None	19.3-19.22, 21.3-21.13	
CVE-2024-21093	Java VM	Create Session, Create Procedure	Oracle Net	No	5.3	Network	High	Low	None	Un-changed	High	None	None	19.3-19.22, 21.3-21.13	
CVE-2024-21058	Unified Audit	SYSDBA	Oracle Net	No	4.9	Network	Low	High	None	Un-changed	None	High	None	19.3-19.22, 21.3-21.13	
CVE-2023-5072	GraalVM Multilingual Engine	None	Multiple	Yes	4.3	Network	Low	None	Required	Un-changed	None	None	Low	21.3-21.13	
CVE-2024-21066	RDBMS	Authenticated User	None	No	4.2	Local	Low	High	Required	Un-changed	High	None	None	19.3-19.22, 21.3-21.13	
CVE-2023-36632	RDBMS (Python)	Authenticated User	Oracle Net	No	3.5	Network	Low	Low	Required	Un-changed	None	None	Low	21.3-21.13	
CVE-2024-20995	Oracle Database Sharding	DBA	Oracle Net	No	2.4	Network	Low	High	Required	Un-changed	None	None	Low	19.3-19.22, 21.3-21.13	

Additional CVEs addressed are:

- The patch for CVE-2023-36632 also addresses CVE-2023-40217, CVE-2023-41105, and CVE-2023-49083.
- The patch for CVE-2023-5072 also addresses CVE-2023-44487, CVE-2024-20918, CVE-2024-20919, CVE-2024-20921, CVE-2024-20922, CVE-2024-20923, CVE-2024-20925, CVE-2024-20926, CVE-2024-20932, CVE-2024-20945, and CVE-2024-20952.

Additional patches included in this Critical Patch Update for the following non-exploitable CVEs for this Oracle product family:

- Core RDBMS (Integrated Performance Primitives): CVE-2023-28823 and CVE-2023-27391 [VEX Justification: vulnerable_code_not_in_execute_path].
- Global Service Manager (Perl): CVE-2023-47038, CVE-2023-47039 and CVE-2023-47100 [VEX Justification: vulnerable_code_cannot_be_controlled_by_adversary].
- Oracle Database Configuration Assistant (Apache Commons Compress): CVE-2023-42503 [VEX Justification: vulnerable_code_not_in_execute_path].
- Oracle Database Gateway for APPC (Perl): CVE-2023-47038, CVE-2023-47039 and CVE-2023-47100 [VEX Justification: vulnerable_code_cannot_be_controlled_by_adversary].
- Oracle Spatial and Graph MapViewer (Apache Xalan-Java): CVE-2022-34169 [VEX Justification: vulnerable_code_not_in_execute_path].
- RDBMS: CVE-2024-23672 and CVE-2024-24549 [VEX Justification: vulnerable_code_not_in_execute_path].
- RDBMS (Dell BSAFE Crypto-J): CVE-2022-34381 and CVE-2023-5363 [VEX Justification: vulnerable_code_not_in_execute_path].
- RDBMS (Perl): CVE-2023-47038, CVE-2023-47039 and CVE-2023-47100 [VEX Justification: vulnerable_code_cannot_be_controlled_by_adversary].
- Security (Kerberos): CVE-2023-39975 [VEX Justification: vulnerable_code_not_present].
- SQLcl (Eclipse parsson): CVE-2023-47038, CVE-2023-47039 and CVE-2023-47100 [VEX Justification: vulnerable_code_cannot_be_controlled_by_adversary].
- Universal Installer (Perl): CVE-2023-47038, CVE-2023-47039 and CVE-2023-47100 [VEX Justification: vulnerable_code_cannot_be_controlled_by_adversary].

Oracle Database Products Risk Matrices

This Critical Patch Update contains 15 new security patches for Oracle Database Products divided as follows:

- 3 new security patches for Oracle Database Products
- 5 new security patches for Oracle Audit Vault and Database Firewall
- 1 new security patch for Oracle Big Data Spatial and Graph
- 3 new security patches for Oracle Essbase
- No new security patches for Oracle Global Lifecycle Management, but third party patches are provided
- 1 new security patch for Oracle GoldenGate
- 1 new security patch for Oracle Graph Server and Client
- 1 new security patch for Oracle NoSQL Database
- No new security patches for Oracle REST Data Services, but third party patches are provided
- No new security patches for Oracle Secure Backup, but third party patches are provided
- No new security patches for Oracle SQL Developer, but third party patches are provided
- No new security patches for Oracle TimesTen In-Memory Database, but third party patches are provided

Oracle Database Server Risk Matrix

This Critical Patch Update contains 3 new security patches, plus additional third party patches noted below, for Oracle Database Products. None of these vulnerabilities may be remotely exploitable without authentication, i.e., none may be exploited over a network without requiring user credentials. None of these patches are applicable to client-only installations, i.e., installations that do not have the Oracle Database Server installed. The English text form of this Risk Matrix can be found here.

CVE ID	Component	Package and/or Privilege Required	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RISK (see Risk Matrix Definitions)									Supported Versions Affected	Notes
					Base Score	Attack Vector	Attack Complex	Privs Req'd	User Interact	Scope	Confid-entiality	Inte-grity	Avail-ability		
CVE-2024-20903	Java VM	Create Session, Create Procedure	Oracle Net	No	6.5	Network	Low	Low	None	Un-changed	None	High	None	19.3-19.21, 21.3-21.12	
CVE-2023-38545	Oracle Spatial and Graph (curl)	Authenticated User	HTTP	No	6.5	Network	Low	Low	None	Un-changed	None	None	High	19.3-19.21, 21.3-21.12, 23.3	
CVE-2022-21432	Oracle Text	DBA	Oracle Net	No	2.7	Network	Low	High	None	Un-changed	None	None	Low	19.3-19.21	

Additional CVEs addressed are:

- The patch for CVE-2023-38545 also addresses CVE-2023-38039 and CVE-2023-38546.

Additional patches included in this Critical Patch Update for the following non-exploitable CVEs for this Oracle product family:

- Grid Infrastructure (Apache Tomcat): CVE-2023-46589, CVE-2023-42794, CVE-2023-42795, CVE-2023-44487 and CVE-2023-45648 [VEX Justification: vulnerable_code_cannot_be_controlled_by_adversary].
- Oracle Autonomous Health Framework (Apache PyArrow): CVE-2023-47248 [VEX Justification: vulnerable_code_cannot_be_controlled_by_adversary].
- Oracle Database Fleet Patching and Provisioning (Apache Derby): CVE-2022-46337 [VEX Justification: vulnerable_code_cannot_be_controlled_by_adversary].
- Oracle Database Workload Manager (Eclipse parsson): CVE-2023-4043 [VEX Justification: vulnerable_code_cannot_be_controlled_by_adversary].
- Oracle Database Workload Manager (Jetty): CVE-2023-40167, CVE-2023-36479 and CVE-2023-41900 [VEX Justification: vulnerable_code_cannot_be_controlled_by_adversary].
- Oracle Notification Server (PCRE2): CVE-2022-41409 [VEX Justification: vulnerable_code_not_in_execute_path].
- SQLcl (Eclipse parsson): CVE-2023-4043 [VEX Justification: vulnerable_code_cannot_be_controlled_by_adversary].
- SQLcl (Google Guava): CVE-2023-2976 [VEX Justification: vulnerable_code_not_in_execute_path].

Oracle Database Products Risk Matrices

This Critical Patch Update contains 20 new security patches for Oracle Database Products divided as follows:

- 10 new security patches for Oracle Database Products
- No new security patches for Oracle Big Data Spatial and Graph, but third party patches are provided
- 1 new security patch for Oracle Essbase
- No new security patches for Oracle Global Lifecycle Management, but third party patches are provided
- 6 new security patches for Oracle GoldenGate
- No new security patches for Oracle Graph Server and Client, but third party patches are provided
- 1 new security patch for Oracle REST Data Services
- 1 new security patch for Oracle Secure Backup
- 1 new security patch for Oracle TimesTen In-Memory Database

Oracle Database Server Risk Matrix

This Critical Patch Update contains 10 new security patches, plus additional third party patches noted below, for Oracle Database Products. 2 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. None of these patches are applicable to client-only installations, i.e., installations that do not have the Oracle Database Server installed. The English text form of this Risk Matrix can be found here.

CVE ID	Component	Package and/or Privilege Required	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RISK (see Risk Matrix Definitions)									Supported Versions Affected	Notes
					Base Score	Attack Vector	Attack Complex	Privs Req'd	User Interact	Scope	Confid-entiality	Inte-grity	Avail-ability		
CVE-2023-38039	Oracle Spatial and Graph (cURL)	Authenticated User	HTTP	No	6.5	Network	Low	Low	None	Un-changed	None	None	High	19.3-19.20, 21.3-21.11	
CVE-2022-44729	Oracle Spatial and Graph (Apache Batik)	Authenticated User	HTTP	No	6.0	Local	Low	High	None	Un-changed	High	None	High	19.3-19.20, 21.3-21.11	
CVE-2022-23491	OML4Py (cryptography)	None	HTTP	Yes	5.9	Network	High	None	None	Un-changed	None	High	None	21.3-21.11	
CVE-2023-22071	PL/SQL	Create Session, Execute on sys.utl_http	Oracle Net	No	5.9	Network	Low	High	Required	Changed	Low	Low	Low	19.3-19.20, 21.3-21.11	
CVE-2023-22077	Oracle Database Recovery Manager	DBA account	Oracle Net	No	4.9	Network	Low	High	None	Un-changed	None	None	High	19.3-19.20, 21.3-21.11	
CVE-2023-22096	Java VM	Create Session, Create Procedure	Oracle Net	No	4.3	Network	Low	Low	None	Un-changed	None	Low	None	19.3-19.20, 21.3-21.11	
CVE-2023-22073	Oracle Notification Server	None	TLS	Yes	4.3	Adjacent Network	Low	None	None	Un-changed	Low	None	None	19.3-19.20, 21.3-21.11	
CVE-2023-35116	Oracle Database Fleet Patching and Provisioning (jackson-databind)	Authenticated User	HTTP	No	3.1	Network	High	Low	None	Un-changed	None	None	Low	19.3-19.20, 21.3-21.11	
CVE-2023-22075	Oracle Database Sharding	Create Session, Create Any View, Select Any Table	Oracle Net	No	2.4	Network	Low	High	Required	Un-changed	None	None	Low	19.3-19.20, 21.3-21.11	
CVE-2023-22074	Oracle Database Sharding	Create Session, Select Any Dictionary	Oracle Net	No	2.4	Network	Low	High	Required	Un-changed	None	None	Low	19.3-19.20, 21.3-21.11	

Oracle Database Products Risk Matrices

This Critical Patch Update contains 15 new security patches for Oracle Database Products divided as follows:

- 5 new security patches for Oracle Database Products
- 3 new security patches for Oracle Application Express
- No new security patches for Oracle Big Data Spatial and Graph, but third party patches are provided
- 2 new security patches for Oracle Essbase
- 2 new security patches for Oracle GoldenGate
- 1 new security patch for Oracle Graph Server and Client
- No new security patches for Oracle NoSQL Database, but third party patches are provided
- No new security patches for Oracle Secure Backup, but third party patches are provided
- 1 new security patch for Oracle Spatial Studio
- 1 new security patch for Oracle TimesTen In-Memory Database

Oracle Database Server Risk Matrix

This Critical Patch Update contains 5 new security patches, plus additional third party patches noted below, for Oracle Database Products. 1 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. 1 of these patches is applicable to client-only installations, i.e., installations that do not have the Oracle Database Server installed. The English text form of this Risk Matrix can be found here.

CVE ID	Component	Package and/or Privilege Required	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RISK (see Risk Matrix Definitions)									Supported Versions Affected	Notes
					Base Score	Attack Vector	Attack Complex	Privs Req'd	User Interact	Scope	Confid-entiality	Inte-grity	Avail-ability		
CVE-2022-43680	Oracle Text (LibExpat)	Create Session, Create Index	Oracle Net	No	6.5	Network	Low	Low	None	Un-changed	None	None	High	19.3-19.19, 21.3-21.10	
CVE-2023-23931	OML4Py (cryptography)	Create Session	Oracle Net	No	5.4	Network	Low	Low	None	Un-changed	None	Low	Low	21.3-21.10	
CVE-2023-22034	Unified Audit	SYSDBA	Oracle Net	No	4.9	Network	Low	High	None	Un-changed	None	High	None	19.3-19.19, 21.3-21.10	
CVE-2023-21949	Advanced Networking Option	None	Oracle Net	Yes	3.7	Network	High	None	None	Un-changed	None	Low	None	19.3-19.19, 21.3-21.10	
CVE-2023-22052	Java VM	Create Session, Create Procedure	Multiple	No	3.1	Network	High	Low	None	Un-changed	None	Low	None	19.3-19.19, 21.3-21.10	

Additional patches included in this Critical Patch Update for the following non-exploitable CVEs for this Oracle product family:

- Core (lz4): CVE-2021-3520 [VEX Justification: vulnerable_code_cannot_be_controlled_by_adversary].
- Oracle Database (Apache Tomcat): CVE-2023-34981, CVE-2022-45143, CVE-2023-24998, CVE-2023-28708 and CVE-2023-28709 [VEX Justification: vulnerable_code_not_present].
- Oracle Database Workload Manager (Dexie): CVE-2022-21189 and CVE-2023-30533 [VEX Justification: vulnerable_code_not_in_execute_path].

Oracle Database Server Client-Only Installations

- The following Oracle Database Server vulnerability included in this Critical Patch Update affects client-only installations: CVE-2023-21949.

Remember to patch all your components

Are you patching all your components:

- OPatch
- Oracle Grid Infrastructure
- Oracle Database Server Home
- Oracle JavaVM Component
- Oracle REST Data Services
- Oracle Application Express
- Autonomous HealthFramework
- .....

An updated ‘Critical Patch Update (CPU) Program Patch Availability Document (DB-only)’ is available for each CPU cycle.

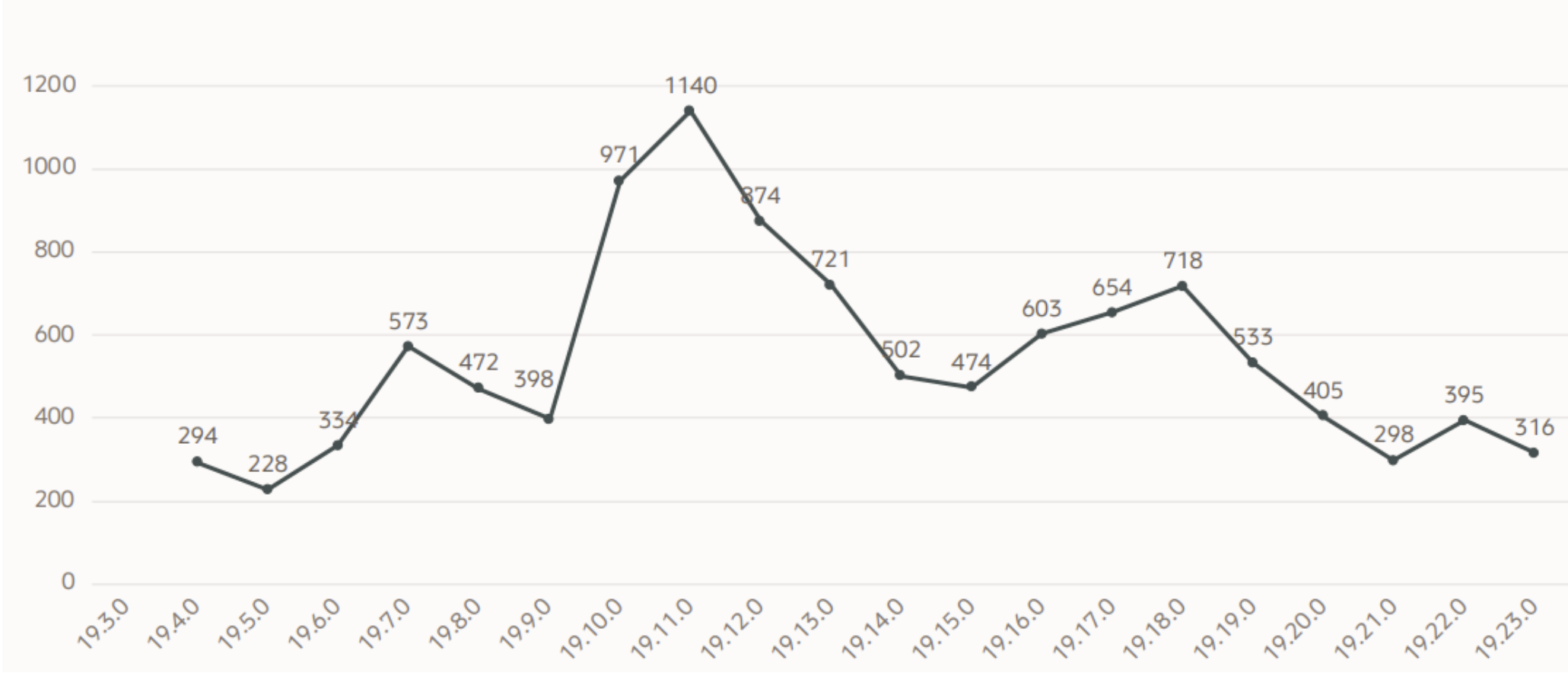
For July 2024:

Critical Patch Update (CPU) Program Jul 2024 Patch Availability Document (DB-only) (Doc ID 3027813.1)

Why MRP / Bundle Patches

Does not only include CPU but also fixes to known bugs.

Database 19 Release Updates and Revisions Bugs Fixed Lists (Doc ID 2523220.1)



itm8

If you are running on Windows

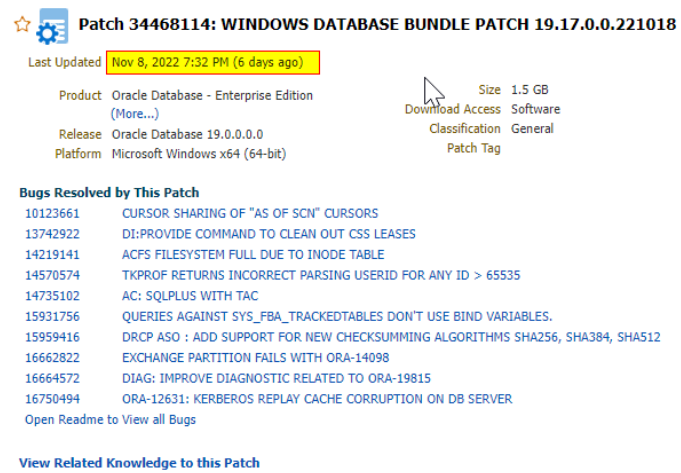
If you are running on Windows or none Linux, patches are often not available before end of month or beginning following month.

ETA for patches are listed in the ‘Post Release Patches’ section of the ‘Patch Availability Document’ and is often subject to change (-> pushed back to later date).

Windows Patches are also often delayed…

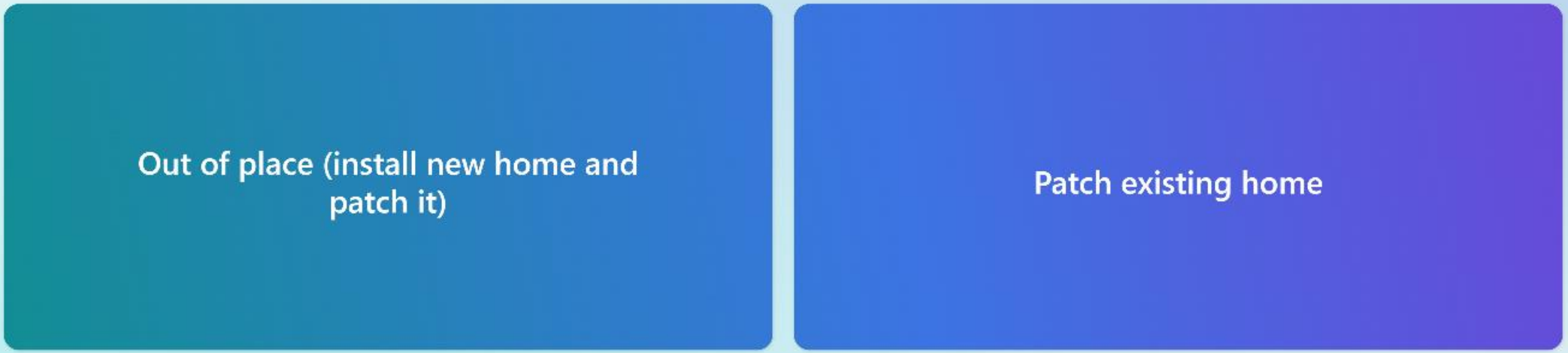
21.8.0.0.221018 WIN BP	Patch 34468137	MS-Windows	05-Nov-2022
19.17.0.0.221018 WIN BP	Patch 34468114	MS-Windows	05-Nov-2022
19.17.0.0.221018 OJVM	Patch 34411846	MS-Windows	05-Nov-2022

21.8.0.0.221018 WIN BP	Patch 34468137	MS-Windows	22-Nov-2022
19.17.0.0.221018 WIN BP	Patch 34468114	MS-Windows	Available
19.17.0.0.221018 OJVM	Patch 34411846	MS-Windows	Available



0 response submitted

How are you patching your Oracle SW HOME?



Treemap Bar

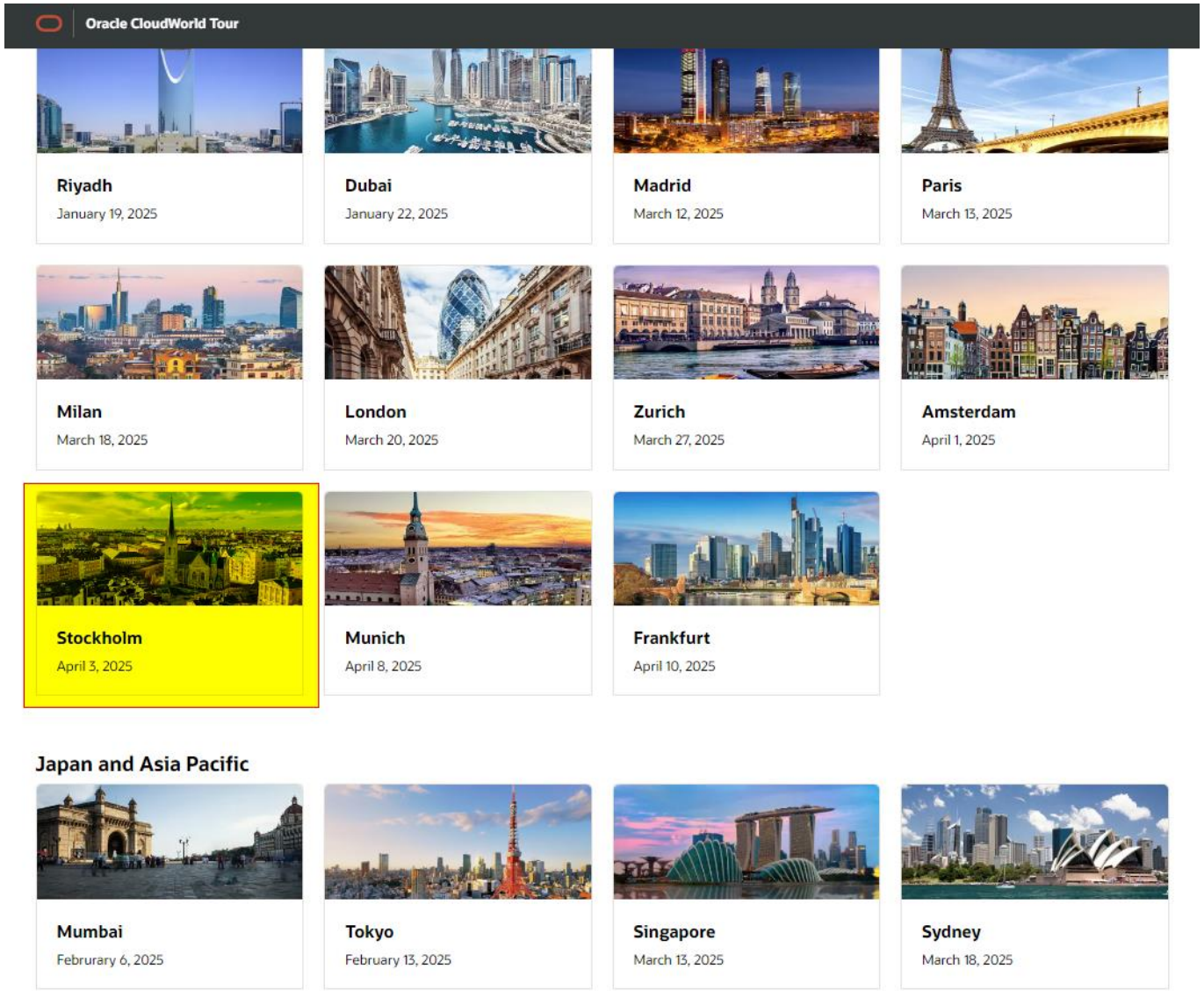
1 of 1

Advantages of out of place patching

Oracle recommends using ‘out of place’ patching for several reasons:

- You can prepare the new home in advance and patch it to the desired level before the downtime window keeping it at a minimal.
- You will have the old home ready if a rollback is needed.
- It will be faster to install the patches since you don’t need to rollback/deinstall previous patches.
- You will keep the size of the home on disk to a minimum since it will not contain the patches installed previously.

Oracle CloudWorld Tour - Stockholm 3rd April



itm8

Good sources for information on upgrades and patching

Mike Dietrich:

https://mikedietrichde.com/

Daniel Overby Hansen:

https://dohdatabase.com/