

Database Patching in the Age of AI and Security Threats

Faster. Easier. Better.

Mike Dietrich - Oracle
Rodrigo Jorge - Oracle
Lucia Hustatyova – Deutsche Telekom Slovakia



Mike Dietrich

Vice President



mikedietrich



@mikedietrichde.com



<https://mikedietrichde.com>



Rodrigo Jorge

Product Management Architect

 [rodrigoaraujorge](#)

 [@dbarj.com.br](#)

 <https://www.dbarj.com.br>



Find Slides and Much More on Our Blogs



MikeDietrichDE.com

Mike.Dietrich@oracle.com



dohdatabase.com

Daniel.Overby.Hansen@oracle.com



DBArj.com.br

Rodrigo.R.Jorge@oracle.com



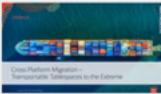
AlexZaballa.com

Alex.Zaballa@oracle.com



axdiaz.com

jorge.a.diaz@oracle.com

Virtual Classroom Seminars	Slides
Episode 16 (replaces Episode 1 from Feb 2021) <u>Oracle Database Release and Patching Strategy for 19c and 23c</u> 115 minutes – May 10, 2023	
Episode 17 <u>From SR to Patch – Insights into the Oracle Database Development process</u> 55 minutes – June 22, 2023	
Episode 18 <u>Cross Platform Migration – Transportable Tablespaces to the Extreme</u> 145 min – February 22, 2024	
Episode 19 <u>Move to Oracle Database 23ai – Everything you need to know about Multitenant PART 1</u> 145 min – May 16, 2024	
Episode 20 <u>Move to Oracle Database 23ai – Everything you need to know about Multitenant PART 2</u> 100 min – June 28, 2024	
Episode 21 <u>One-Button Patching with AutoUpgrade – Easing every DBA's life</u> 55 min – October 24, 2024	

Recorded Web Seminars

<https://MikeDietrichDE.com/videos>

More than 45 hours of technical content
On-demand, anytime, anywhere

Patching 2026



How often do you apply patches?

- Monthly?
- Quarterly?
- Twice a year?
- Once a year?
- Never touch a running system?

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

Critical Patch Updates

Critical Patch Updates provide security patches for supported Oracle on-premises products. A Critical Patch Update is a collection of patches for multiple security vulnerabilities. These patches address vulnerabilities in Oracle code and in third party components included in Oracle products. These patches are usually cumulative. They are available to customers with valid support contracts. Critical Patch Updates are released on the third Tuesday of January, April, July, and October. The next four dates are:

- 19 January 2027
- 20 April 2027
- 20 July 2027
- 19 October 2027

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

The Critical Patch Updates released since 2021 are listed in the following table. Critical Patch Updates released before 2021 are available [here](#).

Critical Patch Update	Latest Version/Date
Critical Patch Update - October 2026	Rev 1, 20 October 2026
Critical Patch Update - July 2026	Rev 7, 20 August 2026
Critical Patch Update - April 2026	Rev 2, 24 April 2026
Critical Patch Update - January 2026	Rev 3, 03 February 2026

Critical Patch Updates

Critical Patch Updates provide security patches for supported Oracle on-premises products. A Critical Patch Update is a collection of patches for multiple security vulnerabilities. These patches address vulnerabilities in Oracle code and in third party components included in Oracle products. These patches are usually cumulative. They are available to customers with valid support contracts. Critical Patch Updates are released on the third Tuesday of January, April, July, and October. The next four dates are:

- 19 January 2027
- 20 April 2027
- 20 July 2027
- 19 October 2027

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

The Critical Patch Updates released since 2021 are listed in the following table. Critical Patch Updates released before 2021 are available [here](#).

Critical Patch Update	Latest Version/Date
Critical Patch Update - October 2026	Rev 1, 20 October 2026
Critical Patch Update - July 2026	Rev 7, 20 August 2026
Critical Patch Update - April 2026	Rev 2, 24 April 2026
Critical Patch Update - January 2026	Rev 3, 03 February 2026

Oracle Critical Patch Update Advisory - October 2026

Description

A Critical Patch Update is a collection of patches for multiple security vulnerabilities. These patches address vulnerabilities in Oracle code and in third party components included in Oracle products. These patches are usually cumulative, but each advisory describes only the security patches added since the previous Critical Patch Update Advisory. Thus, prior Critical Patch Update advisories should be reviewed for information regarding earlier published security patches. Refer to [Critical Patch Updates](#), [Critical Security Patch Updates](#), [Security Alerts and Bulletins](#) for information about Oracle Security advisories.

Oracle continues to periodically receive reports of attempts to maliciously exploit vulnerabilities for which Oracle has already released security patches. In some instances, it has been reported that attackers have been successful because targeted customers had failed to apply available Oracle patches. Oracle therefore strongly recommends that customers remain on actively-supported versions and apply security patches without delay.

This Critical Patch Update contains 1295 new security patches across the product families listed below. Please note that a My Oracle Support (MOS) note summarizing the content of this Critical Patch Update and other Oracle Software Security Assurance activities is located at [October 2026 Critical Patch Update: Executive Summary and Analysis](#).

Affected Products and Patch Information

Security vulnerabilities addressed by this Critical Patch Update affect the products listed below.

Please click on the links in the Patch Availability Document column below to access the documentation for patch availability information and installation instructions.

Oracle Communications Network Analytics Data Director, versions 25.1.200, 25.2.100, 25.2.200	Oracle Communications Network Analytics Data Director
Oracle Communications Operations Monitor, versions 6.0, 6.1	Oracle Communications Operations Monitor
Oracle Communications Policy Management, versions 15.0.0.0.0, 15.1.0.0.0	Oracle Communications Policy Management
Oracle Communications Service Catalog and Design, versions 8.0-8.3	Oracle Communications Service Catalog and Design
Oracle Communications Unified Assurance, versions 6.1.1-7.0.0	Oracle Communications Unified Assurance
Oracle Communications Unified Inventory Management, versions 7.5.0, 7.5.1, 7.6.0, 7.7.0, 7.8.0, 8.0.1	Oracle Communications Unified Inventory Management
Oracle Data Integrator, versions 12.2.1.4.0, 14.1.2.0.0	Fusion Middleware
Oracle Database Server, versions 19.3-19.32, 21.3-21.23, 23.4.0-23.26.3	Database
Oracle Demand Planning, versions 12.1, 12.2	Oracle Supply Chain Products
Oracle E-Business Suite, versions 12.2.3-12.2.15	Oracle E-Business Suite
Oracle Enterprise Manager Base Platform, versions 13.5, 24.1	Oracle Enterprise Manager
Oracle Enterprise Manager for Oracle Database, versions 13.5, 24.1	Oracle Enterprise Manager
Oracle Enterprise Manager for Siebel, versions 13.5, 24.1	Oracle Enterprise Manager
Oracle Enterprise Manager for Virtualization, version 13.5	Oracle Enterprise Manager
Oracle Essbase, version 21.8.3.0.0	Database
Oracle Financial Services Analytical Applications Infrastructure, versions 8.0.7.9, 8.0.8.7, 8.1.2.5, 8.1.2.6	Oracle Financial Services Analytical Applications Infrastructure
Oracle Financial Services Relationship Management	Oracle Financial Services Relationship Management

Oracle Critical Patch Update Advisory - October 2026

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-2026-75803	RDBMS (OpenSSL)	None	TLS	Yes	9.8	Network	Low	None	None	Un- changed	High	High	High	19.3-19.32, 23.4.0-23.26.3	
CVE-2026-91563	Oracle OLAP	DBMS_AW	Oracle Net	No	8.8	Network	Low	Low	None	Un- changed	High	High	High	19.3-19.32, 21.3-21.23, 23.4.0-23.26.3	
CVE-2026-91499	RDBMS	DBMS_VECTOR	Oracle Net	No	8.8	Network	Low	Low	None	Un- changed	High	High	High	23.4.0-23.26.3	
CVE-2026-93569	RDBMS (Micronaut)	None	HTTP	Yes	8.2	Network	Low	None	None	Un- changed	Low	High	None	19.3-19.32, 23.4.0-23.26.3	
CVE-2026-91503	VPD	Create Table	Oracle Net	No	8.1	Network	Low	Low	None	Un- changed	High	High	None	19.3-19.32, 21.3-21.23, 23.4.0-23.26.3	
CVE-2026-91568	RDBMS	Create Session	Oracle Net	No	7.7	Network	Low	Low	None	Changed	High	None	None	23.4.0-23.26.3	
CVE-2026-101512	RDBMS	None	HTTP	No	6.5	Network	Low	Low	None	Un- changed	High	None	None	23.4.0-23.26.3	
CVE-2026-91479	RDBMS	None	UDP	Yes	6.5	Adjacent Network	Low	None	None	Un- changed	None	None	High	23.4.0-23.26.3	
CVE-2026-91615	Java VM	None	SOCKS5	No	6.3	Network	High	Low	None	Changed	None	High	None	19.3-19.32, 21.3-21.23, 23.4.0-23.26.3	

Oracle Critical Patch Update Advisory - October 2026

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-2026-75803	RDBMS (OpenSSL)	None	TLS	Yes	9.8	Network	Low	None	None	Un- changed	High	High	High	19.3-19.32, 23.4.0-23.26.3	
CVE-2026-91563	Oracle OLAP	DBMS_AW	Oracle Net	No	8.8	Network	Low	Low	None	Un- changed	High	High	High	19.3-19.32, 21.3-21.23, 23.4.0-23.26.3	
CVE-2026-91499	RDBMS	DBMS_VECTOR	Oracle Net	No	8.8	Network	Low	Low	None	Un- changed	High	High	High	23.4.0-23.26.3	
CVE-2026-93569	RDBMS (Micronaut)	None	HTTP	Yes	8.2	Network	Low	None	None	Un- changed	Low	High	None	19.3-19.32, 23.4.0-23.26.3	
CVE-2026-91503	VPD	Create Table	Oracle Net	No	8.1	Network	Low	Low	None	Un- changed	High	High	None	19.3-19.32, 21.3-21.23, 23.4.0-23.26.3	
CVE-2026-91568	RDBMS	Create Session	Oracle Net	No	7.7	Network	Low	Low	None	Changed	High	None	None	23.4.0-23.26.3	
CVE-2026-101512	RDBMS	None	HTTP	No	6.5	Network	Low	Low	None	Un- changed	High	None	None	23.4.0-23.26.3	
CVE-2026-91479	RDBMS	None	UDP	Yes	6.5	Adjacent Network	Low	None	None	Un- changed	None	None	High	23.4.0-23.26.3	
CVE-2026-91615	Java VM	None	SOCKS5	No	6.3	Network	High	Low	None	Changed	None	High	None	19.3-19.32, 21.3-21.23, 23.4.0-23.26.3	

Oracle Critical Patch Update Advisory - October 2026

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-2026-75803	RDBMS (OpenSSL)	None	TLS	Yes	9.8	Network	Low	None	None	Un- changed	High	High	High	19.3-19.32, 23.4.0-23.26.3	
CVE-2026-91563	Oracle OLAP	DBMS_AW	Oracle Net	No	8.8	Network	Low	Low	None	Un- changed	High	High	High	19.3-19.32, 21.3-21.23, 23.4.0-23.26.3	
CVE-2026-91499	RDBMS	DBMS_VECTOR	Oracle Net	No	8.8	Network	Low	Low	None	Un- changed	High	High	High	23.4.0-23.26.3	
CVE-2026-93569	RDBMS (Micronaut)	None	HTTP	Yes	8.2	Network	Low	None	None	Un- changed	Low	High	None	19.3-19.32, 23.4.0-23.26.3	
CVE-2026-91503	VPD	Create Table	Oracle Net	No	8.1	Network	Low	Low	None	Un- changed	High	High	None	19.3-19.32, 21.3-21.23, 23.4.0-23.26.3	
CVE-2026-91568	RDBMS	Create Session	Oracle Net	No	7.7	Network	Low	Low	None	Changed	High	None	None	23.4.0-23.26.3	
CVE-2026-101512	RDBMS	None	HTTP	No	6.5	Network	Low	Low	None	Un- changed	High	None	None	23.4.0-23.26.3	
CVE-2026-91479	RDBMS	None	UDP	Yes	6.5	Adjacent Network	Low	None	None	Un- changed	None	None	High	23.4.0-23.26.3	
CVE-2026-91615	Java VM	None	SOCKS5	No	6.3	Network	High	Low	None	Changed	None	High	None	19.3-19.32, 21.3-21.23, 23.4.0-23.26.3	



[Subscribe](#) to email notifications

- Critical Patch Updates and Security Alerts



Why should you patch?

Security Updates

Accelerating Vulnerability Detection and Response at Oracle

April 29, 2026 | 3 minute read



Integrated Cyber Center (ICC)

The latest generation of AI is transforming how software vulnerabilities are identified and fixed, increasing the speed and scale of discovery and remediation.

At Oracle, we have long applied AI across our cloud and software environments to support security testing, vulnerability detection, and code analysis. These capabilities run on Oracle Cloud Infrastructure (OCI), leveraging OCI AI services, infrastructure, and development platforms to operate continuously at scale.

Oracle has access to leading frontier AI models, including Anthropic's Claude Mythos Preview and OpenAI's most capable models through Trusted Access for Cyber, and we are extending our capabilities with these models to improve how quickly and effectively vulnerabilities are identified. Combined with our AI-enabled security operations, these capabilities are applied across Oracle-developed software and services, Oracle Health, and the open-source components we build and use in our products.

The result is stronger code, earlier identification of risk and mitigations, and better protection for Oracle and our



Security Updates

Accelerating Vulnerability Detection and Response at Oracle

April 29, 2026 | 3 min read

Oracle has access to leading frontier AI models, including Anthropic's Claude Mythos Preview and OpenAI's most capable models through Trusted Access for Cyber, and we are extending our capabilities with these models to improve how quickly and effectively vulnerabilities are identified. Combined with our AI-enabled security operations, these capabilities are applied across Oracle-developed software and services, Oracle Health, and the open-source components we build and use in our products.

Oracle has access to leading frontier AI models, including Anthropic's Claude Mythos Preview and OpenAI's most capable models through Trusted Access for Cyber, and we are extending our capabilities with these models to improve how quickly and effectively vulnerabilities are identified. Combined with our AI-enabled security operations, these capabilities are applied across Oracle-developed software and services, Oracle Health, and the open-source components we build and use in our products.

The result is stronger code, earlier identification of risk and mitigations, and better protection for Oracle and our

You must upgrade to Oracle Database 19c or Oracle AI Database 26ai



Everything older must be upgraded **instantly** – no exceptions

You must patch monthly

The world has changed dramatically – this is the new reality



You must upgrade to Oracle Database 19c
or Oracle AI Database 26ai



You must patch your database with the most recent Release Update quarterly



You should **patch monthly**

- Are you ready for it?

[Link](#)

Security Updates

Update: Monthly Critical Security Patch Updates (CSPUs)

Oracle releases security patches on the **third Tuesday of each month**, alternating between **Critical Security Patch Updates (CSPUs)** and **Critical Patch Updates (CPUs)**. [🔗](#) The upcoming release schedule for late 2026 is:

- **October 20, 2026:** Quarterly CPU
- **November 17, 2026:** Monthly CSPU
- **December 15, 2026:** Monthly CSPU
- **January 19, 2027:** Quarterly CPU [🔗](#)

CSPUs are smaller, monthly releases targeting critical vulnerabilities, while **CPUs** are quarterly releases that are cumulative and include all prior CSPU fixes. [🔗](#)

ancing the start date and cadence for

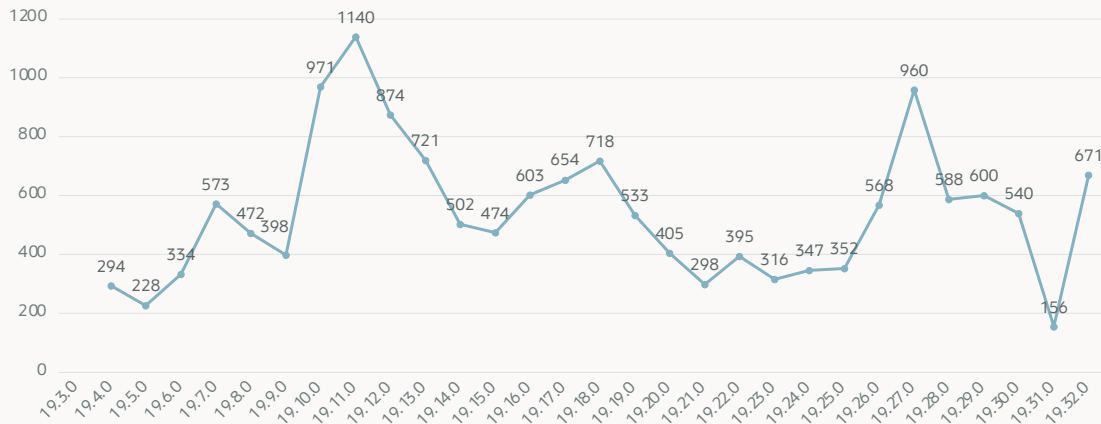
s provide targeted fixes for critical
without waiting for the next quarterly



Release Updates are the primary vehicle for delivering **security** patches

- Plus bug fixes, regression fixes and more

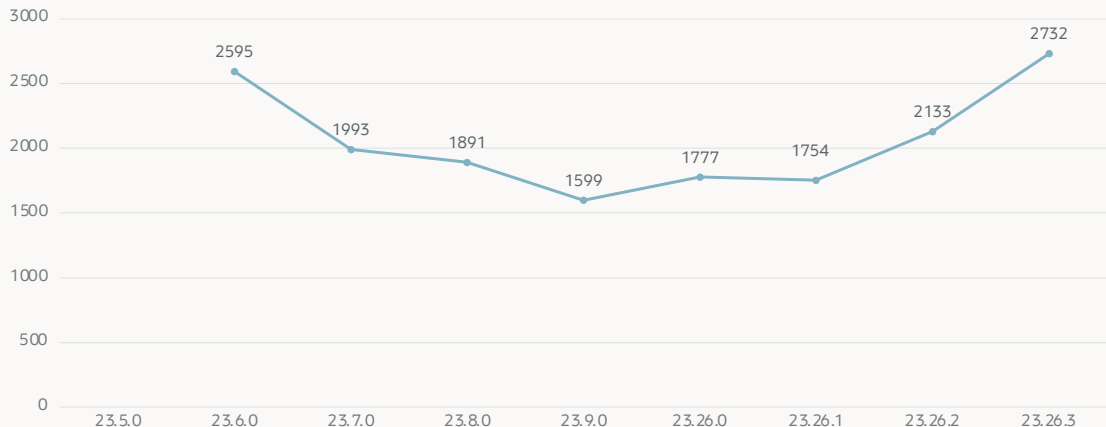
Release Update Contents – Oracle Database 19c



[Database 19 Release Updates and Revisions Bugs Fixed Lists \(KB850150\)](#)



Release Update Contents – Oracle AI Database 26ai



Source: oradiff.oracle.com





How many security fixes get shipped?

*Let's ask
Rodrigo Jorge*

oradiff.oracle.com

RU Security Patches – Oracle Database 19.32.0 ➔ 19.33.0

Oracle Release Analyzer Diff Utility

MOS Account | Settings | Help | rodrigo.r.jorge@oracle.com

- Home
- Parameters
- Users, Roles, etc
- Privileges
- Included Fixes
 - List of Fixes
 - Total Fixes
 - Search Fixes
 - List of CVEs
 - CPU Explore
 - Fix Control
- Oracle Database Home
- Objects
- Fixed Objects

Bug Id	Patch Id	Bug Description
39249975	39915792	Fix for Bug 39249975
39250461	39915792	Fix for Bug 39250461

Fix for Bug 39253861

Fix for Bug 39254307

Fix for Bug 39256249

Fix for Bug 39258682

Fix for Bug 39259173

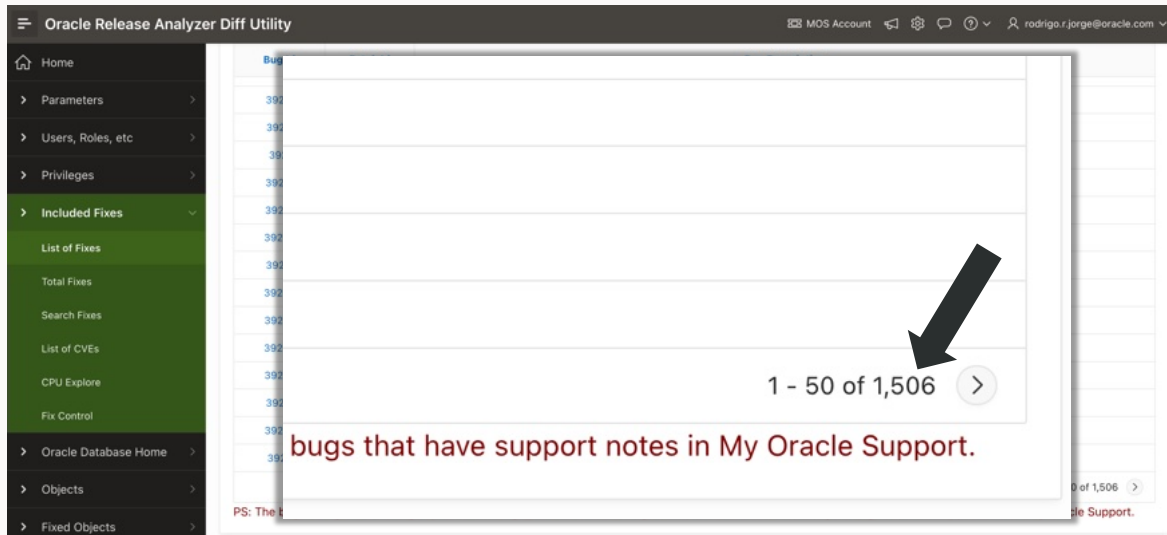
1 - 50 of 702 >

links will be valid only for bugs that have support notes in My Oracle Support.

PS: The bug links generated using system.out.print Bug Fixes, Components, Bug Information and Bug Fix List only for bugs that have support notes in My Oracle Support.



RU Security Patches – Oracle Database 23.26.3 → 23.26.4



The screenshot displays the Oracle Release Analyzer Diff Utility interface. The left sidebar contains a navigation menu with the following items: Home, Parameters, Users, Roles, etc, Privileges, Included Fixes (expanded), List of Fixes, Total Fixes, Search Fixes, List of CVEs, CPU Explore, Fix Control, Oracle Database Home, Objects, and Fixed Objects. The main content area shows a table of bugs, with the first column labeled 'Bug'. A modal overlay is present in the center, displaying a pagination control '1 - 50 of 1,506' and a right arrow button. A large black arrow points to the right arrow button. Below the pagination control, the text 'bugs that have support notes in My Oracle Support.' is displayed in red. The bottom of the modal shows a partial view of the bug list, including the text 'PS: The t' and 'le Support.'

Oracle Release Analyzer Diff Utility

MOS Account

rodrigo.r.jorge@oracle.com

Home

Parameters

Users, Roles, etc

Privileges

Included Fixes

List of Fixes

Total Fixes

Search Fixes

List of CVEs

CPU Explore

Fix Control

Oracle Database Home

Objects

Fixed Objects

Bug

1 - 50 of 1,506

bugs that have support notes in My Oracle Support.

PS: The t

le Support.



If you don't apply a recent Release Update, you will miss **thousands** of **security fixes**

- In total, almost 2,200 security fixes on 19.33.0
- In total, almost 4,000 security fixes on 23.26.4

Older Release Updates?

File Download

Click each file name to download the selected files.

Tip: Use a Download Manager [Learn More...](#)

DATABASE RELEASE UPDATE 19.28.0.0.0(Patch:Linux x86)

 **p37960098_190000_LINUX.zip** (299.3 MB)

Why a Password?



Unlock

Total Size 299.3 MB

Download File Metadata

View Digest Details

Download wget Script

Close

Quarterly Release Updates

	2024				2025				2026				2027		
	January	April	July	October	January	April	July	October	January	April	July	October	January	April	July
19c	19.22.0	19.23.0	19.24.0	19.25.0	19.26.0	19.27.0	19.28.0	19.29.0	19.30.0	19.31.0	19.32.0	19.33.0	19.34.0	19.35.0	19.36.0
21c	21.13.0	21.14.0	21.15.0	21.16.0	21.17.0	21.18.0	21.19.0	21.20.0	21.21.0	21.22.0	21.23.0	21.24.0	21.25.0	21.26.0	21.27.0
26ai			23.5.0	23.6.0	23.7.0	23.8.0	23.9.0	23.26.0	23.26.1	23.26.2	23.26.3	23.26.4	23.27.1	23.27.2	23.27.3



Monthly Recommended Patches

Linux only for Oracle Database 19c and Oracle AI Database 26ai

	2026												2027	
	January	February	March	April	May	June	July	August	September	October	November	December	January	February
19.30.0	19.30.0	MRP1	MRP2	MRP3	MRP4	MRP5	MRP6							
19.31.0				19.31.0	MRP1	MRP2	MRP3	MRP4	MRP5	MRP6				
19.32.0							19.32.0	MRP1	MRP2	MRP3	MRP4	MRP5	MRP6	
19.33.0										19.33.0	MRP1	MRP2	MRP3	MRP4



Critical Security Patch Updates

On all platforms except Linux for 19c and 26ai

	2026												2027	
	January	February	March	April	May	June	July	August	September	October	November	December	January	February
19.30.0	19.30.0						CSPU1							
19.31.0				19.31.0	MRP1	MRP2	CSPU1	CSPU2	CSPU3	CSPU4				
19.32.0							19.32.0	CSPU1	CSPU2	CSPU3	CSPU4	CSPU5	CSPU6	
19.33.0										19.33.0	CSPU1	CSPU2	CSPU3	CSPU4



Content

MRP – Monthly Recommended Patch

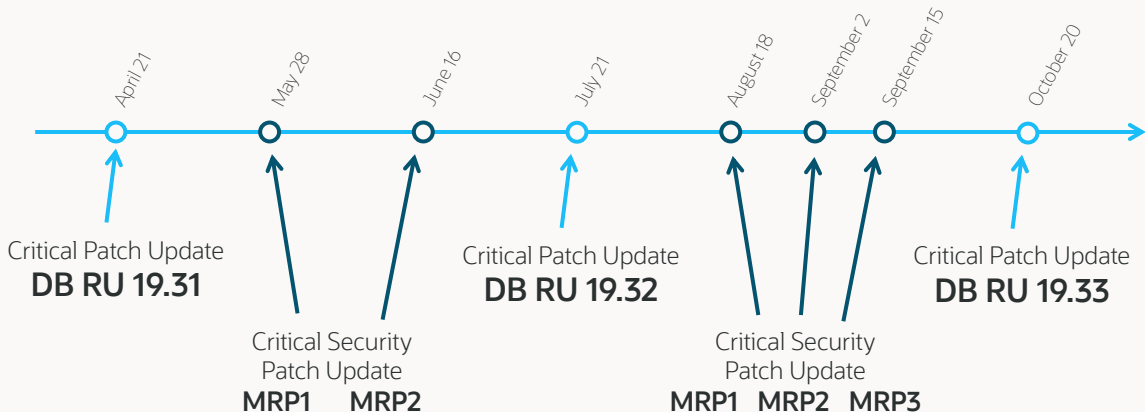
- [KB188772](#)
 - Critical fixes
 - Regression fixes
 - 3rd party tools security fixes
- Security fixes

CSPU – Critical Security Patch Update

- Critical fixes
- Security fixes



Patching Best Practices





MRPs and CSPUs will co-exist

- MRPs on Linux for Oracle 19c and 26ai
- CSPUs on all other platforms, and for Oracle 21c

Please wake up. This is **real!!**

Patching Oracle AI Database

1

DOWNLOAD

2

INSTALL

3

PATCH

4

FINALIZE



Downloading patches *still* the old way?

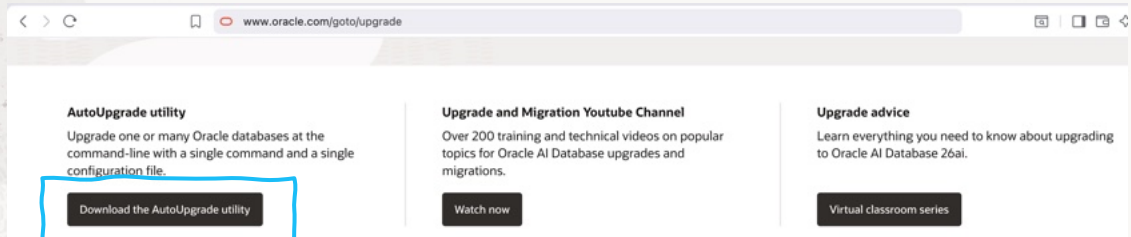


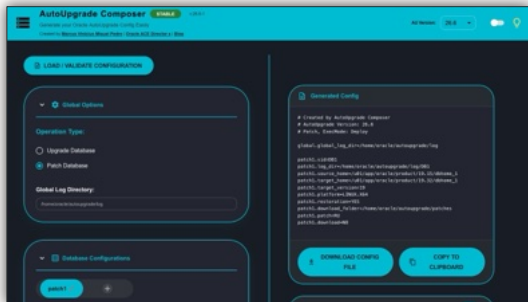
Easiest way to download patches and install them? **Use AutoUpgrade!!**

- One single tool for all platforms
- Always, take the newest

- Always use the latest version of AutoUpgrade
- Available via direct download from [oracle.com](https://www.oracle.com) or [KB123450](#)

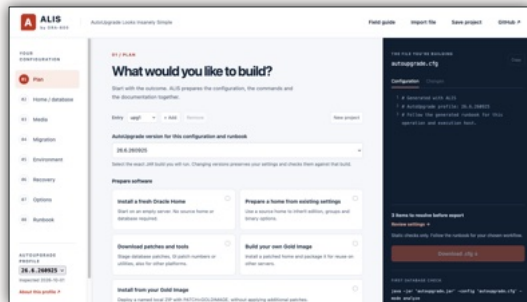
```
wget https://download.oracle.com/otn-pub/otn_software/autoupgrade.jar
```





AutoUpgrade Composer

<https://autoupgrade-composer.com>



ALIS

<https://ora600pl.github.io/alis>



Marcus Vinicius Miguel Pedro

ACE Director



Kamil Stawiarski

ACE Director

```
global.global_log_dir=/home/oracle/autoupgrade-patching/log
```



```
global.global_log_dir=/home/oracle/autoupgrade-patching/log  
global.keystore=/home/oracle/autoupgrade-patching/keystore
```



Learn how to configure the keystore in our previous webinar

- [One-Button Patching – makes life easier for every Oracle DBA](#)

```
global.global_log_dir=/home/oracle/autoupgrade-patching/log  
global.keystore=/home/oracle/autoupgrade-patching/keystore  
global.download_folder=/home/oracle/autoupgrade/patches
```

```
global.global_log_dir=/home/oracle/autoupgrade-patching/log  
global.keystore=/home/oracle/autoupgrade-patching/keystore  
global.download_folder=/home/oracle/autoupgrade/patches
```

```
patch1.target_version=19
```

```
global.global_log_dir=/home/oracle/autoupgrade-patching/log  
global.keystore=/home/oracle/autoupgrade-patching/keystore  
global.download_folder=/home/oracle/autoupgrade/patches
```

```
patch1.target_version=19  
patch1.platform=LINUX.X64
```

```
global.global_log_dir=/home/oracle/autoupgrade-patching/log  
global.keystore=/home/oracle/autoupgrade-patching/keystore  
global.download_folder=/home/oracle/autoupgrade/patches
```

```
patch1.target_version=19  
patch1.platform=LINUX.X64  
patch1.patch=RU
```

```
$ opatch apply
```

```
Oracle Interim Patch Installer version 12.2.0.1.17  
Copyright (c) 2025, Oracle Corporation. All rights reserved.
```

```
...
```

```
The OPatch being used has version 12.2.0.1.17 while the following patch(es)  
require higher versions:
```

```
Patch 38291812 requires OPatch version 12.2.0.1.47.
```

```
Please download latest OPatch from My Oracle Support.
```

```
global.global_log_dir=/home/oracle/autoupgrade-patching/log  
global.keystore=/home/oracle/autoupgrade-patching/keystore  
global.download_folder=/home/oracle/autoupgrade/patches
```

```
patch1.target_version=19  
patch1.platform=LINUX.X64  
patch1.patch=RU,OPATCH
```



Consume the most important fixes for known issues, regressions and security

- MRPs on Linux for Oracle 19c and 26ai
- CSPUs for Oracle 21c and on all non-Linux ports

```
global.global_log_dir=/home/oracle/autoupgrade-patching/log  
global.keystore=/home/oracle/autoupgrade-patching/keystore  
global.download_folder=/home/oracle/autoupgrade/patches
```

```
patch1.target_version=19  
patch1.platform=LINUX.X64  
patch1.patch=RU,OPATCH,MRP
```



Apply the OJVM bundle patch

```
global.global_log_dir=/home/oracle/autoupgrade-patching/log  
global.keystore=/home/oracle/autoupgrade-patching/keystore  
global.download_folder=/home/oracle/autoupgrade/patches
```

```
patch1.target_version=19  
patch1.platform=LINUX.X64  
patch1.patch=RU,OPATCH,MRP,OJVM
```



OJVM is embedded in Release Updates

- No separate download
- Complete RAC Rolling patching support



Don't miss out on all the Data Pump fixes

```
global.global_log_dir=/home/oracle/autoupgrade-patching/log  
global.keystore=/home/oracle/autoupgrade-patching/keystore  
global.download_folder=/home/oracle/autoupgrade/patches
```

```
patch1.target_version=19  
patch1.platform=LINUX.X64  
patch1.patch=RU,OPATCH,MRP,OJVM,DPBP
```



What about AutoUpgrade itself?

```
global.global_log_dir=/home/oracle/autoupgrade-patching/log  
global.keystore=/home/oracle/autoupgrade-patching/keystore  
global.download_folder=/home/oracle/autoupgrade/patches
```

```
patch1.target_version=19  
patch1.platform=LINUX.X64  
patch1.patch=RU,OPATCH,MRP,OJVM,DPBP,AU
```

```
global.global_log_dir=/home/oracle/autoupgrade-patching/log
global.keystore=/home/oracle/autoupgrade-patching/keystore
global.download_folder=/home/oracle/autoupgrade/patches
```

```
patch1.target_version=19
patch1.platform=LINUX.X64
patch1.patch=RU,OPATCH,MRP,OJVM,DPBP,AU
patch1.patch=RECOMMENDED
```

Recommended Patches

`patch1.patch=RECOMMENDED`

OPATCH

The latest OPatch

RU

The latest Release Update

OJVM

OJVM bundle matching Release Update

DPBP

Data Pump bundle patch matching RU

AU

Latest version of AutoUpgrade

MRP/CSPU

Latest available MRP/CSPU for this RU



Apply latest JDK patch

```
$ORACLE_HOME/jdk/bin/java -version
```

```
java version "1.8.0_471"
```

```
Java(TM) SE Runtime Environment (build 1.8.0_471-b09)
```

```
Java HotSpot(TM) 64-Bit Server VM (build 25.471-b09, mixed mode)
```




```
global.global_log_dir=/home/oracle/autoupgrade-patching/log  
global.keystore=/home/oracle/autoupgrade-patching/keystore  
global.download_folder=/home/oracle/autoupgrade/patches
```

```
patch1.target_version=19  
patch1.platform=LINUX.X64  
patch1.patch=RECOMMENDED, JDK
```



Apply other patches
via patch number

Apply the Most Important Patches - [KB188772](#) / 555.1

Recommended Patches for 19.31 DB Home

Below is the list of important patches to consider applying on top of 19.31.

Special Note: As of 5/15/2026 Oracle Database 19.31 has been re-released due to an issue affecting environments running Exadata Software Release 25.2. and Oracle Database 19.31. For more information see Note [KB888427](#).*

Bug	KM Article	Fixed in RU	Fixed in MRP	Description	Patches	RAC Rolling Installable	Database Online Installable	Added
39370763	KB888427		DBMRP 19.31.0.0.260519	[OSS SRV LAYER] DB56: Disable Flash Cache Temp Reuse and ASM Partner Read in 19.31 (one off)	PATCH 39370763	YES	NO	14-MAY-2026
38238416 (replaces 37690446)	KI40882			[SQL EXECUTION] Bug 38238416 - ORA-600 [ktatmkref-rs] with RAC roll option for 19c	PATCH 38238416	YES	NO	30-APR-2026
38723830 (replaces 34672698)	KI55221	Not Eligible	Not Eligible	[VOS] DB50: ORA-800: soft external error, arguments: [set priority failed], [vktm] , dism(16) or ORA-7445 [__intel_sse2_strncmp()+379]	PATCH 38723830	YES	NO	31-MAR-2026
34774667	KI36203	Not Eligible	Not Eligible	[AQ] ORA-7445 in Purge Queue Table / High CPU usage in SVCB Service	PATCH 34774667	NO	NO	11-JUL-2023
29213893	KI24589	Not Eligible	Not Eligible	[QRY OPTIMIZER] DBMS_STATS Failing With Error Ora-1422 When Gathering Stats for User\$ Table	PATCH 29213893	NO	NO	01-SEP-2021

Version DB 19.31_555.1: 39370763,38238416,38723830,34774667,29213893

```
global.global_log_dir=/home/oracle/autoupgrade-patching/log  
global.keystore=/home/oracle/autoupgrade-patching/keystore  
global.download_folder=/home/oracle/autoupgrade/patches
```

```
patch1.target_version=19  
patch1.platform=LINUX.X64  
patch1.patch=RECOMMENDED,JDK,38238416
```



Apply product-specific bundle patches
based on your usage

Oracle Database Patches to Consider for 19c

KA912

Last Updated
Feb 17, 2026



1.4

Getting
Started

Perform
ance

Golden
Gate

Oracle
Text

Platform
Specific

Data Guard High
Availability

DN
FS

Data
Pump

Partitio
ning

Multite
nant

Gene
ral

Oracle
Spatial

Search This Document

Print

Getting Started

When applying Database patches, Oracle recommends that you take a 3-tiered step-by-step approach.

LEVEL 1: Apply latest quarterly patches:

- Apply latest quarterly updates using [Master Note for Database Proactive Patch Program \(Doc ID KB106822\)](#)

LEVEL 2: Apply Critical/Recommended patches:

- For Exadata environments: [Exadata Critical Issues \(KB623062\)](#)
- For Database environments:
 - Customers on Linux x86-64 - Apply the latest Monthly Recommended Patches - MRP (FAQ2283) for the specific RU
 - For customers on other platforms, apply critical patches using Oracle Database 19c Important Recommended One-off Patches (KB858385)

LEVEL 3: Apply additional patches based on features or focus areas:

- Use the tabs in this document for quick access to additional feature based patches

Article Feedback



Rate this

```
global.global_log_dir=/home/oracle/autoupgrade-patching/log  
global.keystore=/home/oracle/autoupgrade-patching/keystore  
global.download_folder=/home/oracle/autoupgrade/patches
```

```
patch1.target_version=19  
patch1.platform=LINUX.X64
```

```
patch1.patch=RECOMMENDED,JDK,38238416,SDOBP
```

```
global.global_log_dir=/home/oracle/autoupgrade-patching/log  
global.keystore=/home/oracle/autoupgrade-patching/keystore  
global.download_folder=/home/oracle/autoupgrade/patches
```

```
patch1.target_version=19  
patch1.platform=LINUX.X64
```

```
patch1.patch=RECOMMENDED,JDK,38238416,SDOBP,TEXT
```



Any other bundle patch
AutoUpgrade should download?



Patch the OCW component

```
$ORACLE_HOME/OPatch/opatch lspatches
```

```
38632161;Database Release Update : 19.30.0.0.260120(REL-JAN260130) (38632161)  
29585399;OCW RELEASE UPDATE 19.3.0.0.0 (29585399)
```





It is mandatory to update OCW with
Oracle RAC Database and Oracle Restart

- In the database Oracle home

```
global.global_log_dir=/home/oracle/autoupgrade-patching/log  
global.keystore=/home/oracle/autoupgrade-patching/keystore  
global.download_folder=/home/oracle/autoupgrade/patches
```

```
patch1.target_version=19  
patch1.platform=LINUX.X64  
patch1.patch=RECOMMENDED,JDK,OCW
```

```
$ORACLE_HOME/OPatch/opatch lspatches
```

```
38632161;Database Release Update : 19.30.0.0.260120(REL-JAN260130) (38632161)
```

```
38661284;OCW RELEASE UPDATE 19.30.0.0.0 (38661284)
```





AutoUpgrade downloads the GI RU
- use it to patch Grid Infrastructure

i

What else?

```
global.global_log_dir=/home/oracle/autoupgrade-patching/log  
global.keystore=/home/oracle/autoupgrade-patching/keystore  
global.download_folder=/home/oracle/autoupgrade/patches
```

```
patch1.target_version=19  
patch1.platform=LINUX.X64  
patch1.patch=AHF,CVU,SQLCL,CPAT,DBSAT
```

```
global.global_log_dir=/home/oracle/autoupgrade-patching/log  
global.keystore=/home/oracle/autoupgrade-patching/keystore  
global.download_folder=/home/oracle/autoupgrade/patches
```

```
patch1.target_version=19  
patch1.platform=LINUX.X64  
patch1.patch=EXAQFSDP:19,EXAPATCHMGR
```



```
global.global_log_dir=/home/oracle/autoupgrade-patching/log  
global.keystore=/home/oracle/autoupgrade-patching/keystore  
global.download_folder=/home/oracle/autoupgrade/patches
```

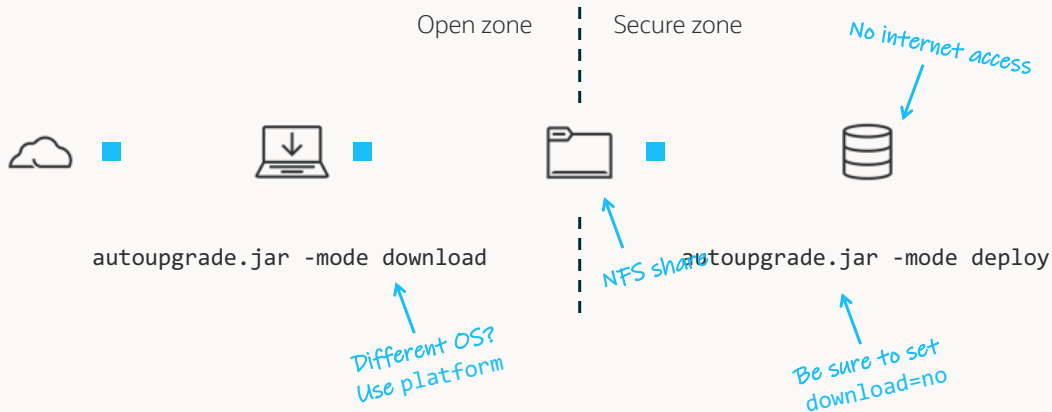
```
patch1.platform=LINUX.X64  
patch1.target_version=19  
patch1.patch=OEM:13.5
```

```
patch2.platform=LINUX.X64  
patch2.target_version=19  
patch2.patch=OEM:24.1
```



Your database host
doesn't have internet access?

Using Download Mode



Using Proxy to Download Patches

```
$ export https_proxy='https://proxy.example.com:8080'
```

```
$ java -jar autoupgrade.jar ... -mode download
```



Let's download some patches

```
global.global_log_dir=/home/oracle/autoupgrade-patching/log  
global.keystore=/home/oracle/autoupgrade-patching/keystore  
global.download_folder=/home/oracle/autoupgrade/patches
```

```
patch1.target_version=19
```

```
patch1.platform=LINUX.X64
```

```
patch1.patch=RECOMMENDED,MRP,38854064,37690446,34672698,34774667,29213893,SDOBP,TEXT,JDK,OCW
```

```
global.global_log_dir=/home/oracle/autoupgrade-patching/log  
global.keystore=/home/oracle/autoupgrade-patching/keystore  
global.download_folder=/home/oracle/autoupgrade/patches
```

```
patch1.target_version=19  
patch1.platform=LINUX.X64  
patch1.patch=RECOMMENDED,MRP,38854064,37690446,34672698,34774667,29213893,SDOBP,TEXT,JDK,OCW
```

```
patch2.target_version=19  
patch2.platform=AIX.X64  
patch2.patch=RECOMMENDED,JDK,OCW
```

```
global.global_log_dir=/home/oracle/autoupgrade-patching/log
global.keystore=/home/oracle/autoupgrade-patching/keystore
global.download_folder=/home/oracle/autoupgrade/patches
```

```
patch1.target_version=19
patch1.platform=LINUX.X64
patch1.patch=RECOMMENDED,MRP,38854064,37690446,34672698,34774667,29213893,SDOBP,TEXT,JDK,OCW
```

```
patch2.target_version=19
patch2.platform=AIX.X64
patch2.patch=RECOMMENDED,JDK,OCW
```

```
patch3.target_version=26
patch3.platform=LINUX.X64
patch3.patch=RECOMMENDED,JDK,OCW
```

-- Start AutoUpgrade in download mode to get the patches specified in the config file

```
java -jar autoupgrade.jar -config get.cfg -mode download
```



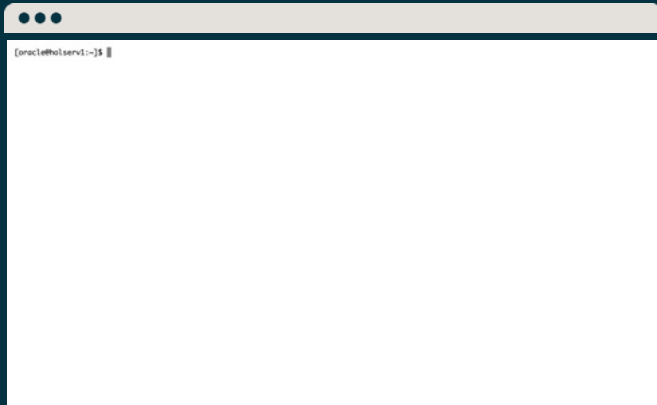
DEMO

Download patches

- Multiple releases
- Multiple platforms



[Watch on YouTube](#)



1

DOWNLOAD

2

INSTALL

3

PATCH

4

FINALIZE



Always patch Out-of-Place

- Don't argue with us 😊

```
cat install19.cfg
```

```
global.global_log_dir=/home/oracle/autoupgrade-patching/log  
global.download_folder=/home/oracle/autoupgrade/patches  
patch1.source_home=/u01/app/oracle/product/dbhome_19_32 ← Settings  
patch1.target_home=/u01/app/oracle/product/dbhome_19_33  
patch1.patch=RECOMMENDED
```

↑
Patches

```
cat install19.cfg
```

```
global.global_log_dir=/home/oracle/autoupgrade-patching/log  
global.download_folder=/home/oracle/autoupgrade/patches  
patch1.source_home=/u01/app/oracle/product/dbhome_19_32  
patch1.target_home=/u01/app/oracle/product/dbhome_19_33  
patch1.patch=RECOMMENDED
```

```
java -jar autoupgrade.jar -config install19.cfg -mode create_home
```



Override source home setting

```
global.global_log_dir=/home/oracle/autoupgrade-install/log  
global.download_folder=/home/oracle/autoupgrade/patches
```

```
patch1.source_home=/u01/app/oracle/product/dbhome_19_32  
patch1.target_home=/u01/app/oracle/product/dbhome_19_33  
patch1.patch=RECOMMENDED  
patch1.home_settings.home_name=OraDbHome1933
```



```
global.global_log_dir=/home/oracle/autoupgrade-install/log  
global.download_folder=/home/oracle/autoupgrade/patches
```

```
patch1.source_home=/u01/app/oracle/product/dbhome_19_32  
patch1.target_home=/u01/app/oracle/product/dbhome_19_33  
patch1.patch=RECOMMENDED  
patch1.home_settings.home_name=OraDbHome1933  
patch1.home_settings.binopt.part=no
```

```
global.global_log_dir=/home/oracle/autoupgrade-install/log  
global.download_folder=/home/oracle/autoupgrade/patches
```

```
patch1.source_home=/u01/app/oracle/product/dbhome_19_32  
patch1.target_home=/u01/app/oracle/product/dbhome_19_33  
patch1.patch=RECOMMENDED  
patch1.home_settings.home_name=OraDbHome1933  
patch1.home_settings.binopt.part=no  
patch1.home_settings.binopt.uniaud=yes
```





Works with Oracle RAC databases, too!

- Automatically detected
- No additional configuration

Build and use Gold Images



Download
Patches



Build
Gold Image



Deploy / Install
Gold Image



Patch

```
cat buildGoldImage.cfg
```

```
global.global_log_dir=/home/oracle/autoupgrade-patching/log  
global.download_folder=/home/oracle/autoupgrade/patches
```

```
buildgold1.source_home=/u01/app/oracle/product/dbhome_19_32  
buildgold1.target_home=/u01/app/oracle/product/dbhome_19_33  
buildgold1.create_gold_image=db_home_1933.zip  
buildgold1.patch=RECOMMENDED
```



```
cat buildGoldImage.cfg
```

```
global.global_log_dir=/home/oracle/autoupgrade-patching/log  
global.download_folder=/home/oracle/autoupgrade/patches
```

```
buildgold1.source_home=/u01/app/oracle/product/dbhome_19_32  
buildgold1.target_home=/u01/app/oracle/product/dbhome_19_33  
buildgold1.create_gold_image=db_home_1933.zip  
buildgold1.patch=RECOMMENDED
```

```
java -jar autoupgrade.jar -config buildGoldImage.cfg -mode create_home
```

```
cat installGoldImage.cfg
```

```
global.global_log_dir=/home/oracle/autoupgrade-patching/log  
global.download_folder=/home/oracle/autoupgrade/patches
```

```
installgold1.source_home=/u01/app/oracle/product/dbhome_19_32  
installgold1.target_home=/u01/app/oracle/product/dbhome_19_33  
installgold1.patch=GOLDIMAGE:db_home_1933.zip
```

```
cat installGoldImage.cfg
```

```
global.global_log_dir=/home/oracle/autoupgrade-patching/log  
global.download_folder=/home/oracle/autoupgrade/patches
```

```
installgold1.source_home=/u01/app/oracle/product/dbhome_19_32  
installgold1.target_home=/u01/app/oracle/product/dbhome_19_33  
installgold1.patch=GOLDIMAGE:db_home_1933.zip
```

```
java -jar autoupgrade.jar -config installGoldImage.cfg -mode create_home
```

1

DOWNLOAD

2

INSTALL

3

PATCH

4

FINALIZE



Patch a single instance database

global.global_log_dir=/home/oracle/autoupgrade-patch/log

patch1.sid=CDB19

patch1.source_home=/u01/app/oracle/product/dbhome_19_32

patch1.target_home=/u01/app/oracle/product/dbhome_19_33



-- Patch the database according to the specification in the config file
-- This takes care of all the necessary steps, including pre- and post-tasks

java -jar autoupgrade.jar -config CDB19.cfg -mode **deploy**



Rolling patch apply on Oracle RAC Database

```
global.global_log_dir=/home/oracle/autoupgrade-patch/log
```

```
patch1.sid=CDB19
```

```
patch1.source_home=/u01/app/oracle/product/dbhome_19_32
```

```
patch1.target_home=/u01/app/oracle/product/dbhome_19_33
```

```
patch1.rac_rolling=auto
```



Default value

`patch1.rac_rolling`

DISABLED

Patch using non-rolling method
(outage)

REQUIRED

Patch using rolling method or stop
if non-rolling patches are detected

AUTO

Automatically detects the best approach
([default](#))

FORCE

Force using rolling method



AutoUpgrade stops the service using the default drain timeout

- But we give you more control

```
global.global_log_dir=/home/oracle/autoupgrade-patching/log
```

```
patch1.sid=CDB191
```

```
patch1.source_home=/u01/app/oracle/product/dbhome_19_31
```

```
patch1.target_home=/u01/app/oracle/product/dbhome_19_32
```

```
patch1.rac_rolling=auto
```

```
patch1.drain_timeout=300
```



```
global.global_log_dir=/home/oracle/autoupgrade-patch/log
```

```
patch1.sid=CDB19
```

```
patch1.source_home=/u01/app/oracle/product/dbhome_19_32
```

```
patch1.target_home=/u01/app/oracle/product/dbhome_19_33
```

```
patch1.rac_rolling=auto
```

```
patch1.drain_timeout=WAIT
```



drain_timeout

patch1.drain_timeout = WAIT

```
srvctl relocate service  
-oldinst node1  
-stopoption TRANSACTIONAL  
-drain_timeout 2592000  
-wait yes  
-verbose
```

> proceed -job 101

```
srvctl stop instance  
-instance node1  
-stopoption IMMEDIATE  
-drain_timeout 0  
-failover  
-verbose  
-force
```

patch1.drain_timeout = 120

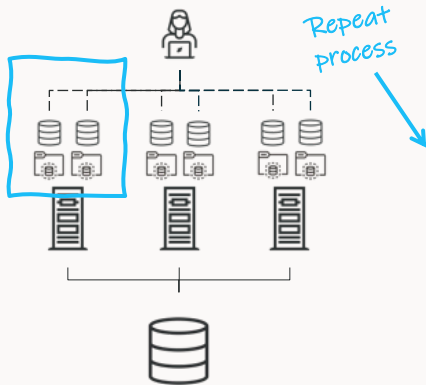
```
srvctl stop instance  
-instance node1  
-stopoption IMMEDIATE  
-drain_timeout 120  
-failover  
-verbose  
-force
```

patch1.drain_timeout (unset)

```
srvctl stop instance  
-instance node1  
-stopoption IMMEDIATE  
-failover  
-verbose  
-force
```

↑
When unset, value used
will be the MAX drain
of all running services
on that instance.

Controlling the Draining



```
autoupgrade.jar ... -mode deploy
```

```
srvctl relocate service \  
-stopoption TRANSACTIONAL \  
-drain_timeout 2592000 ...
```

```
upg> proceed -job 101
```

```
srvctl srvctl stop instance \  
-stopoption IMMEDIATE \  
-drain_timeout 0 ...
```



Patching Data Guard

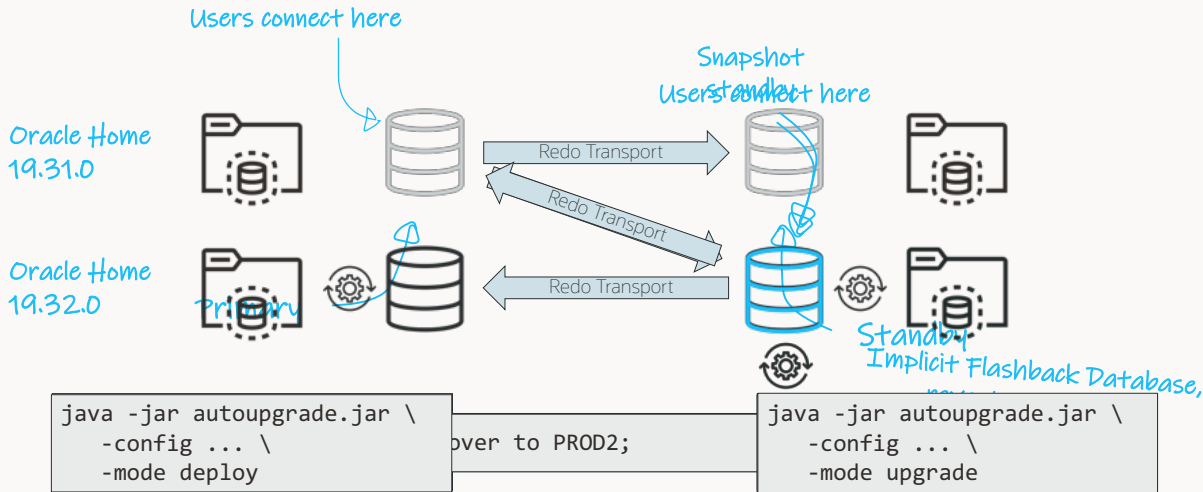


Reduce downtime to the time it takes
to perform a switchover



Safely test and verify patches with
Standby-First Patch Apply

Standby-First Patching





Patch must Standby-First installable

- RUs, MRPs and CSPUs are always Standby-First installable

Is your Oracle Home fully patched?

Check it with AutoUpgrade 26.7
using the Oracle Update Advisor



Add patch?



Replace patch?



Remove patch?



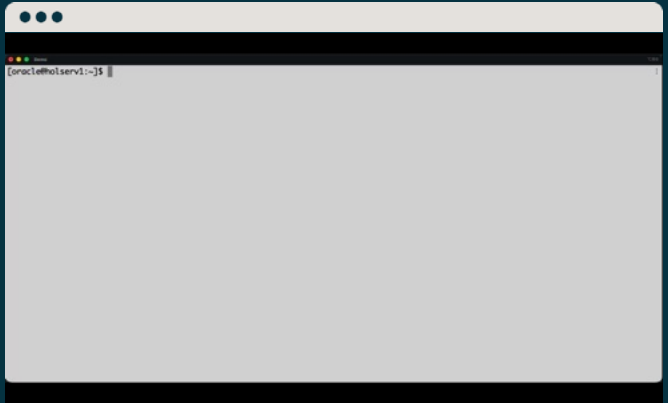
You patched yesterday ...



... but today is another day!!

DEMO

Check Status



 [Watch on YouTube](#)

1

DOWNLOAD

2

INSTALL

3

PATCH

4

FINALIZE



Don't forget the clients

Oracle Critical Patch Update Advisory - October 2026

Description

A Critical Patch Update is a collection of patches for multiple security vulnerabilities. These patches address vulnerabilities in Oracle code and in third party components included in Oracle products. These patches are usually cumulative, but each advisory describes only the security patches added since the previous Critical Patch Update Advisory. Thus, prior Critical Patch Update advisories should be reviewed for information regarding earlier published security patches. Refer to [Critical Patch Updates](#), [Critical Security Patch Updates](#), [Security Alerts and Bulletins](#) for information about Oracle Security advisories.

Oracle continues to periodically receive reports of attempts to maliciously exploit vulnerabilities for which Oracle has already released security patches. In some instances, it has been reported that attackers have been successful because targeted customers had failed to apply available Oracle patches. Oracle therefore strongly recommends that customers remain on actively-supported versions and apply security patches without delay.

This Critical Patch Update contains 1295 new security patches across the product families listed below. Please note that a My Oracle Support (MOS) note summarizing the content of this Critical Patch Update and other Oracle Software Security Assurance activities is located at [October 2026 Critical Patch Update: Executive Summary and Analysis](#).

Affected Products and Patch Information

Security vulnerabilities addressed by this Critical Patch Update affect the products listed below.

Please click on the links in the Patch Availability Document column below to access the documentation for patch availability information and installation instructions.



Every quarter, you should evaluate the need for client patching

- Establish a structured process

AutoUpgrade

Patching automation. Easy. Fast. Reliable.

AutoUpgrade

1. Download patches
2. Create gold image
3. Install home
4. Patch database (incl RAC Rolling)

Reality Check



Deutsche Telekom Slovakia

Oracle AI World 2026

Deutsche Telekom
IT Solutions
Slovakia

ORACLE DATABASES

Oracle Database Patching

From 19c to 26ai — patching at scale in Deutsche Telekom



DEUTSCHE TELEKOM IT SOLUTIONS SLOVAKIA

RNDr. Lucia Hustatyova, MBA

Enterprise Architect

Oct-2026

ABOUT THE SPEAKER

Lucia Hustatyova



ENTERPRISE ARCHITECT · SENIOR DBA

Deutsche Telekom IT Solutions Slovakia

I design highly available Oracle architectures and automate the operations around them.

FOCUS MAA · Data Guard · RAC · Exadata · GoldenGate · Patching · Migrations · Upgrades · TDE · Automation · REST API automation

BLOG <https://www.luciahustatyova.com>

THREE BOOKS



Oracle AI Database
23/26ai



GoldenGate
Microservices



MAA with GoldenGate
HUB

Certifications

Triple Oracle Certified Master (10g, 11g, 12c), Exadata specialist, cloud AI certifications.

Oracle ACE Pro

WomenTech Network
Ambassador for Slovakia.



Sharing knowledge

Blogger, author and speaker at
conferences and universities.

Academic Board

Academic Board Member responsible for
reviewing and approving IT program
accreditation changes.

4,000

employees at Deutsche Telekom IT Solutions Slovakia,
in Košice



>200k

employees across Deutsche Telekom, in more than 40
countries



#1

ICT employer in Slovakia



Why patching matters more in the AI era

FASTER THREATS

AI accelerates vulnerability discovery and exploitation. The window between disclosure and attack is shrinking.

MORE DATA AT STAKE

AI brings vectors, enterprise data and business context closer together. Protecting the database protects the AI foundation.

BROADER ATTACK SURFACE

Vector Search, Select AI agents and new integrations introduce more functionality — and more components to secure.

Trusted AI starts with a trusted, patched database.

Patching is required, not only recommended

01

Customers

02

Auditors

03

Between cycles

04

Evidence

Patching is routine, and automation made it scale

1000+

Databases in every patch cycle.

4× / YEAR

Quarterly RU as the standard baseline.

≤30 DAYS

Target from release to production for relevant high-risk vulnerabilities.

~200h

Hands-on work per cycle, down from ~1000h.

~80%

Manual steps removed by Ansible orchestration and AutoUpgrade.

19c → 26ai

Every production database is on 19c multitenant, with 26ai adoption started.

From patching activity to patching factory

01

Multiple versions

11g / 12c / 19c



Standardized platform

19c multitenant, moving toward 26ai

02

Custom patching

Individual scripts/playbooks



Standardized automation

Ansible + AutoUpgrade + gold images

03

In-place

Patch existing home



Out-of-place

Build and switch to a new Oracle Home

04

Maintenance outage

Maintenance windows



Availability-aware patching

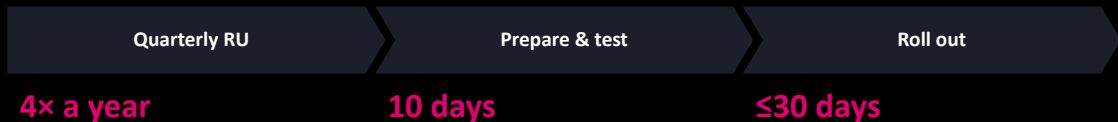
RAC rolling / Data Guard standby-first

Standardization made automation possible. Automation made scale possible.

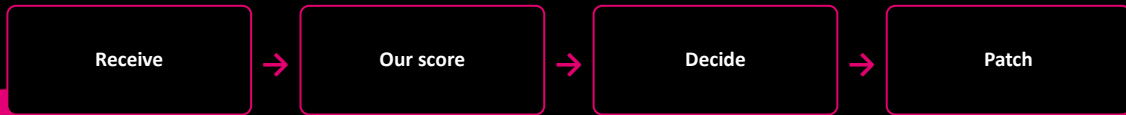
OUR PATCHING PROCESS

Quarterly by default, urgent CVEs evaluated separately

REGULAR PATCHING · EVERY QUARTER



EVALUATION · EVERY REPORTED CVE, OUTSIDE THE REGULAR CYCLE



DECISION

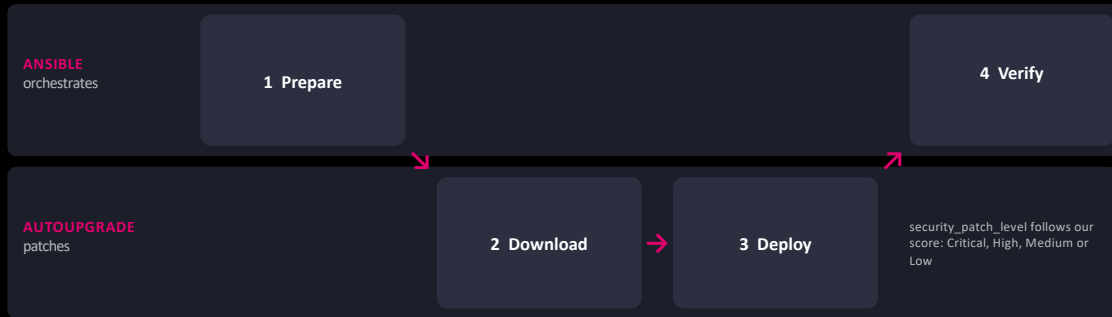
When we apply the patch: 8 is high, 9 is out-of-band

Calculated score	What we do	AutoUpgrade gold image level
9.0 - 10.0 Critical	Out-of-band patch	SecurityCritical
7.0 - 8.9 High (e.g. 8.2)	Next scheduled cycle	SecurityHigh
4.0 - 6.9 Medium	Next quarterly cycle	SecurityMedium
0.1 - 3.9 Low	Regular RU	SecurityLow
Actively exploited	Treated as Critical	SecurityCritical

How we score: Oracle's CVSS base score from the CPU risk matrix, adjusted for our setup (databases are internal only, e.g. 9.1 becomes 8.2). The calculated score sets the deadline.

Gold images: AutoUpgrade gold images use the same levels. We set security_patch_level from the calculated score.

Ansible orchestrates, AutoUpgrade patches



NEAR-ZERO DOWNTIME · SAFE FALLBACK

RAC rolling patching

Data Guard standby-first

One CDB patch, every PDB

Old home + rollback / restore

26ai changes the database, not our patching

01

SAME CADENCE

02

SAME TOOLS

03

SAME SAFETY

04

SAME EVIDENCE

New release, same process.

*26ai doesn't change how we patch —
it increases the need to make patching routine, automated and measurable.*

Three takeaways

01 Patch regularly, **react by score**

Quarterly RU as the baseline. Each reported CVE is scored: 7+ in 30 days, 9+ out-of-band.

02 Automate **consistency**, not only execution

Same image. Same checks. Same process. Same evidence.

03 Design for **patchability**

RAC, Data Guard, multitenant, out-of-place: low downtime, always a way back.



THANK YOU



DEUTSCHE TELEKOM IT SOLUTIONS SLOVAKIA

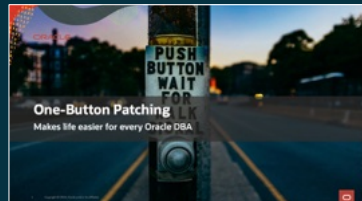
Webinar

One-Button Patching

Makes life easier for every Oracle DBA

Recording on [YouTube](#)

Get the [slides](#)



Patch smarter, not harder

Makes life easier for every Oracle DBA

Recording on [YouTube](#)

Get the [slides](#)



Hands-on Lab

Patch Me If You Can

It's better to fail in our lab, than in production



[Access lab on Oracle Live Labs](#)

Help shape our future events. Get rewarded.

- 1 Download the Oracle Events app**
- 2 Share your feedback in-app**
Scan the QR Code and complete all qualifying surveys
- 3 Earn a giveaway**
Proceed to the Swag Station in the Hub after completing your surveys



In-app surveys

ORACLE