DigiTalk

ORACLE

Critical Patch Updates & Critical Security Patch Updates

A Comprehensive Guide to Oracle's Quarterly and Higher-Frequency Security Patch Programs

Compiled from Oracle's official Security Alerts page

Source: oracle.com/security-alerts

Document current as of 29 July 2026

DigiTalk

Table of Contents

1. Introduction

Oracle publishes security fixes for its on-premises products through a set of formal, scheduled and unscheduled advisory mechanisms. These are documented on Oracle's official Critical Patch Updates, Security Alerts and Bulletins page.

This guide focuses in particular on Oracle's two scheduled patching programs — the long-standing quarterly Critical Patch Update (CPU) and the newly introduced, higher-frequency Critical Security Patch Update (CSPU) — and explains how they fit together with Oracle's other advisory mechanisms: Security Alerts, Solaris Third Party Bulletins, and Oracle Linux Security Advisories.

> **In Short:** Oracle now operates two complementary scheduled patch programs: the quarterly Critical Patch Update (CPU), running since long before 2021, and the new Critical Security Patch Update (CSPU), first released on 28 May 2026, which fills the gaps between quarterly CPU releases with smaller, targeted updates roughly every month.

2. Critical Patch Updates (CPU) — The Quarterly Program

2.1 What Is a Critical Patch Update?

A Critical Patch Update (CPU) is a collection of patches for multiple security vulnerabilities, addressing issues in both Oracle's own code and third-party components bundled with Oracle products. CPUs are usually cumulative, meaning each new CPU generally includes the fixes from previous updates as well as new ones. They are available to customers with valid support contracts and cover Oracle's full portfolio of supported on-premises products.

2.2 Release Cadence

Critical Patch Updates are released on the third Tuesday of January, April, July, and October — four times per year. A pre-release announcement is published on the Thursday preceding each CPU release, giving customers advance notice of which product families will be affected (without revealing vulnerability specifics).

Upcoming CPU Release Dates

Release	Date
Critical Patch Update — July 2026	21 July 2026
Critical Patch Update — October 2026	20 October 2026
Critical Patch Update — January 2027	19 January 2027
Critical Patch Update — April 2027	20 April 2027

Historical CPU Releases (2021 – 2026)

The table below lists every Critical Patch Update released since 2021, along with its most recent revision and date. Earlier releases are available in Oracle's CPU archive.

Critical Patch Update	Latest Version / Date
CPU — July 2026 (Pre-Release Announcement)	Pre-Release
CPU — April 2026	Rev 2, 24 Apr 2026
CPU — January 2026	Rev 3, 02 Feb 2026
CPU — October 2025	Rev 1, 21 Oct 2025
CPU — July 2025	Rev 4, 28 Jul 2025
CPU — April 2025	Rev 2, 21 Apr 2025
CPU — January 2025	Rev 2, 11 Feb 2025
CPU — October 2024	Rev 2, 25 Nov 2024
CPU — July 2024	Rev 3, 18 Sep 2024

Critical Patch Update	Latest Version / Date
CPU — April 2024	Rev 2, 18 Sep 2024
CPU — January 2024	Rev 5, 11 Feb 2025
CPU — October 2023	Rev 5, 8 Dec 2023
CPU — July 2023	Rev 1, 18 Jul 2023
CPU — April 2023	Rev 2, 25 Apr 2023
CPU — January 2023	Rev 3, 27 Feb 2023
CPU — October 2022	Rev 3, 12 Dec 2022
CPU — July 2022	Rev 4, 31 Oct 2022
CPU — April 2022	Rev 9, 23 Dec 2024
CPU — January 2022	Rev 7, 23 Dec 2024
CPU — October 2021	Rev 3, 18 Jan 2022
CPU — July 2021	Rev 7, 03 Sep 2021
CPU — April 2021	Rev 6, 28 Jul 2021
CPU — January 2021	Rev 3, 22 Feb 2021

Revision Behavior: *Some CPUs receive multiple revisions well after their original release date (for example, the April 2022 and January 2022 CPUs were last revised in December 2024). Always check the latest revision of an advisory rather than relying on the original release date alone.*

3. Critical Security Patch Updates (CSPU) — The New Higher-Frequency Program

3.1 What Is a Critical Security Patch Update?

A Critical Security Patch Update (CSPU) is a newer Oracle advisory type that provides targeted, high-priority security fixes in a smaller, more focused format than a full quarterly CPU, making them easier to apply with minimal disruption. CSPUs complement — rather than replace — Oracle's existing quarterly cumulative Critical Patch Updates. Like CPUs, they are available to customers with valid support contracts.

3.2 Why Oracle Introduced CSPUs

The quarterly CPU cadence can leave a gap of up to three months between scheduled fixes for a given product. The Critical Security Patch Update program was introduced to shrink that gap: by releasing smaller, targeted patch sets in most of the months that fall between CPU releases, Oracle can get high-priority fixes to customers considerably faster, without waiting for the next full quarterly cycle.

3.3 Release Cadence

The first Critical Security Patch Update was released on 28 May 2026. CSPUs are released on the third Tuesday of February, March, May, June, August, September, November, and December — eight times per year. A pre-release announcement is published on the Thursday preceding each CSPU release, beginning in June 2026.

Upcoming CSPU Release Dates

Release	Date
Critical Security Patch Update — August 2026	18 August 2026
Critical Security Patch Update — September 2026	15 September 2026
Critical Security Patch Update — November 2026	17 November 2026
Critical Security Patch Update — December 2026	15 December 2026

CSPU Releases to Date

Critical Security Patch Update	Latest Version / Date
CSPU — June 2026	Rev 1, 16 Jun 2026
CSPU — May 2026 (first release)	Rev 1, 28 May 2026

DigiTalk

4. Combined Release Cadence — CPU and CSPU Together

Taken together, the quarterly CPU and the eight-times-a-year CSPU give Oracle a scheduled security release in nearly every month of the year. It is not accurate to call either program individually "monthly" — CPU is quarterly and CSPU is eight-times-yearly — but the two programs interleave so that, from 2026 onward, customers can expect a scheduled Oracle security release in ten or eleven months of any given year.

2026 – 2027 Combined Release Calendar

Month	Program	Status
January 2026	Critical Patch Update	Released
February 2026	—	No scheduled release (CSPU program not yet started)
March 2026	—	No scheduled release (CSPU program not yet started)
April 2026	Critical Patch Update	Released
May 2026	Critical Security Patch Update	Released (program launch)
June 2026	Critical Security Patch Update	Released
July 2026	Critical Patch Update	Pre-release announced; release due 21 Jul 2026
August 2026	Critical Security Patch Update	Scheduled — 18 Aug 2026
September 2026	Critical Security Patch Update	Scheduled — 15 Sep 2026
October 2026	Critical Patch Update	Scheduled — 20 Oct 2026
November 2026	Critical Security Patch Update	Scheduled — 17 Nov 2026
December 2026	Critical Security Patch Update	Scheduled — 15 Dec 2026
January 2027	Critical Patch Update	Scheduled — 19 Jan 2027
February 2027	Critical Security Patch Update	Expected (pattern-based; not yet formally announced)
March 2027	Critical Security Patch Update	Expected (pattern-based; not yet formally announced)
April 2027	Critical Patch Update	Scheduled — 20 Apr 2027

Forward-Looking Dates: *From February and March 2027 onward, dates follow the announced day-of-week pattern (third Tuesday) but have not yet been formally published by Oracle as of this writing. Always confirm against the live Oracle Security Alerts page before relying on a future date.*

DigiTalk

CPU vs. CSPU — Quick Comparison

Attribute	Critical Patch Update (CPU)	Critical Security Patch Update (CSPU)
Program start	Long-running (pre-2021 archive exists)	28 May 2026 (first release)
Frequency	Quarterly — 4 times / year	8 times / year
Release day	3rd Tuesday of Jan, Apr, Jul, Oct	3rd Tuesday of Feb, Mar, May, Jun, Aug, Sep, Nov, Dec
Scope	Broad, cumulative fixes across the full product portfolio	Smaller, targeted, high-priority fixes
Relationship	Primary, comprehensive quarterly baseline	Complements CPU; fills the gaps between quarters
Pre-release announcement	Thursday before release	Thursday before release (from Jun 2026)
Eligibility	Valid support contract required	Valid support contract required

5. Security Alerts — Out-of-Band Emergency Fixes

Separately from the scheduled CPU and CSPU programs, Oracle issues Security Alerts for vulnerability fixes considered too critical to wait for the next scheduled release. These are published as soon as a fix is ready, independent of the quarterly or higher-frequency calendar.

Security Alerts Released Since 2021

Security Alert	Latest Version / Date
Alert for CVE-2026-35273	Rev 1, 10 Jun 2026
Alert for CVE-2026-21992	Rev 2, 20 Mar 2026
Alert for CVE-2025-61884	Rev 1, 11 Oct 2025
Alert for CVE-2025-61882	Rev 2, 06 Oct 2025
Alert for CVE-2024-21287	Rev 1, 18 Nov 2024
Alert for CVE-2022-21500	Rev 2, 25 May 2022
Alert for CVE-2021-44228 (Log4Shell)	Rev 3, 17 Dec 2021

> **Example:** *CVE-2021-44228 corresponds to the widely known "Log4Shell" vulnerability in Apache Log4j, illustrating that Security Alerts are reserved for industry-wide critical issues, not routine product-specific bugs.*

6. Related Bulletins and Advisories

6.1 Solaris Third Party Bulletins

Solaris Third Party Bulletins announce security patches for third-party software distributed with Oracle Solaris. They are published on the same day as the quarterly CPU, and are typically updated once between quarterly cycles — or sooner, for critical fixes.

Solaris Third Party Bulletin	Latest Version / Date
Bulletin — April 2026	Rev 2, 16 Jun 2026
Bulletin — January 2026	Rev 3, 18 Mar 2026
Bulletin — October 2025	Rev 3, 16 Dec 2025
Bulletin — July 2025	Rev 3, 23 Sep 2025
Bulletin — April 2025	Rev 3, 18 Jun 2025

Earlier bulletins (back to 2021) are available in Oracle's Solaris bulletin archive on the source page.

6.2 Oracle Linux Security Advisories

Security advisories for Oracle Linux are published on a separate, dedicated site rather than the main Security Alerts page:

https://linux.oracle.com/security/

7. CVE Mapping and Additional Resources

- Map of CVE to Advisory/Alert — indicates which CVEs are fixed in each CPU, CSPU, and Security Alert.

https://www.oracle.com/in/security-alerts/public-vuln-to-advisory-mapping.html

- Map of CVE to Solaris Third Party Bulletin — indicates which CVEs are fixed in each Solaris bulletin.

https://www.oracle.com/in/security-alerts/public-vuln-to-bulletin-mapping.html

- Oracle CVEs not published in other Oracle public documents.

https://www.oracle.com/in/security-alerts/all-oracle-cves-outside-other-oracle-public-documents.html

8. Oracle's Disclosure Policy

As a matter of policy, Oracle does not provide additional information about the specifics of a vulnerability beyond what is included in the CPU, CSPU, or Security Alert notification, the pre-installation notes, the readme files, and FAQs.

- Oracle provides all customers with the same information at the same time, to protect all customers equally.
- Oracle does not provide advance notification or "insider information" to individual customers.
- Oracle does not distribute exploit code or proof-of-concept code for vulnerabilities in its products.

9. Applicability to Oracle Cloud

Oracle Cloud operations and security teams regularly evaluate CPU, CSPU, and Security Alert fixes — along with relevant third-party fixes — as they become available, and apply the relevant patches in accordance with Oracle's internal change management processes.

Customers needing information not addressed in a specific advisory can obtain it as follows:

- Oracle Cloud (IaaS, PaaS, SaaS) customers — submit a Service Request (SR) within their designated support system.
- Oracle Managed Cloud Services (OMCS) customers — contact their Service Delivery Manager (SDM) or Technical Account Manager (TAM).
- CRM On Demand customers — request status via a Service Request (SR).
- Global Business Units / Industry Cloud Services customers — submit an SR, or contact their Customer Success Manager if applicable.
- Oracle Advertising customers — contact their Client Partner.
- Oracle NetSuite customers — submit a Support Case from within their Oracle NetSuite account.

DigiTalk

10. References and Further Reading

- Oracle Software Security Assurance

https://www.oracle.com/in/corporate/security-practices/assurance/

- Oracle's Policy and Process for Fixing Security Vulnerabilities

https://www.oracle.com/in/corporate/security-practices/assurance/vulnerability/security-fixing.html

- Guidelines for Reporting Security Vulnerabilities

https://www.oracle.com/in/corporate/security-practices/assurance/vulnerability/reporting.html

- Oracle Corporate Security Blog

https://blogs.oracle.com/security/

- Instructions for Subscribing to Email Notifications

https://www.oracle.com/in/security-alerts/securityemail.html

- Original Source Page — Critical Patch Updates, Security Alerts and Bulletins

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