SAP and ERP: is the system that moves your money patched, closed and watched?

This month, take every ERP web component that doesn't need to be public off the internet, and apply each month's SAP Security Notes and Oracle patches within the patching sheet's deadlines. Then close the paths inside (RFC gateway, trusted connections, standard users, SAP_ALL in production) and keep the Security Audit Log on and in your SIEM, so someone reviews every emergency and admin session.

Reviewed	Next review	Version
5 Nov 2026	**5 Dec 2026**	**1.0**

Written for
SAP Basis, security and IT teams running SAP ECC, S/4HANA, RISE or BTP, and teams running Oracle or Microsoft ERP systems

Latest version
sheets.einblick.dev/sap-erp/

If you only do five things

1. **Take ERP web components off the internet.** Publish only the HTTP paths partners need, through a reverse proxy in front of SAP Web Dispatcher[12], and never the SAP GUI, gateway, message server or start service ports[15].
2. **Patch every month, by exploitation and exposure.** SAP releases Security Notes on the second Tuesday of each month[1], and Oracle now patches monthly[9]. A ransomware group weaponized an SAP NetWeaver flaw a day after disclosure[6].
3. **Keep support packages under 24 months old.** SAP fixes new high and critical notes only for support packages shipped in the last 24 months[1].
4. **Lock down the RFC gateway.** Use SAP's restrictive secinfo and reginfo files[16], and store no passwords in RFC connections from development to production[12].
5. **Take SAP_ALL out of production.** BSI allows SAP_ALL, SAP_NEW and S_DEVELOP change rights there only for logged emergency users[12]. Turn on the Security Audit Log in all clients[25].

Handle each SAP Patch Day

1. **Which notes apply to which system?** System Recommendations in SAP Solution Manager matches new Security Notes and HotNews against each system[2]; otherwise filter All Security Notes in SAP for Me[1].
2. **How fast must each one go in?** Use the patching sheet's tiers: exploited (in KEV[5]) within 72 hours on internet-facing systems and 7 days inside, other Critical and High notes within 14 and 30 days.
3. **Did the fix reach production?** Implement ABAP corrections in development, transport them on[28] and record each note's status per system[12].
4. **Is the server still talking to the internet?** Block non-essential outbound internet traffic from ERP servers, as Google advises for EBS; it can disrupt an attack even after a break-in[7].

Exploited ERP flaws since 2025

- **SAP Visual Composer, CVE-2025-31324 and -42999.** Ransomware used both uploader flaws; in KEV since 29 April and 15 May 2025[5].
- **Oracle EBS, CVE-2025-61882.** Google saw likely zero-day attacks from 9 August 2025 and data theft[7]; in KEV since 6 October[5].
- **Oracle PeopleSoft, CVE-2026-35273.** ShinyHunters exploited it from 27 May 2026, before Oracle's 10 June alert[8]; in KEV since 12 June[5].
- **Oracle Payments in EBS, CVE-2026-46817.** An unauthenticated takeover rated 9.8, fixed on 28 May 2026[11]; in KEV since 15 July[5].

Close the paths inside

- **Block function modules nobody calls.** In UCON's final phase, remote-enabled function modules not assigned to a communication assembly can't be called from outside[17].
- **Treat trusted RFC like a stored password.** We extend BSI's stored-password rule[12]: production never trusts development or test systems.
- **Lock the standard users.** Lock SAP*, DDIC and EARLYWATCH but keep SAP* in every client, and check with report RSUSR003[18].
- **Run jobs as technical users.** Background jobs run as System users, not Dialog users[12]. Move the transport job RDDIMPDP off DDIC, so DDIC can stay locked[18].

Powerful rights and emergency access

- **Remove debug and replace.** S_DEVELOP for DEBUG with change rights lets users alter accounting data in memory, bypassing the audit trail[14].
- **Remove all-table access.** No production user should display every table through SE16 with S_TABU_DIS for all groups[14].
- **Review every firefighter session.** Unlock emergency users per ticket and log everything[12]. SAP Access Control sends each session's logs to a reviewer, if the system records them[19].
- **Protect vendor bank details.** Mark bank fields as sensitive, so a second user must confirm changes before the automatic payment run[20]; manual payments aren't blocked[21].

Logs, transports and custom code

- **Send the audit log to your SIEM.** Microsoft Sentinel for SAP charges per production system and needs SAP Integration Suite[24,25].
- **Gate every transport.** Build roles and code only in development[12]; the ABAP Test Cockpit checks code at transport release[22]. Its security checks, Code Vulnerability Analyzer, need a per-user license on premises or a BTP ABAP Environment[23].

When ERP security fixes stop

- **End of 2027.** Mainstream maintenance ends for SAP ERP 6.0, EHP 6 to 8[26], and SAP Solution Manager[2].
- **2028 to 2030.** Optional extended maintenance, at 2 percentage points more[26]. Then, in customer-specific maintenance, SAP considers new high and critical notes for 12 months only[1].

- **Follow APP.4.6 in custom ABAP.** Check AUTHORITY-CHECK results; avoid dynamic Open SQL, ADBC and INSERT REPORT[13].

What to demand from RISE and partners

- **Know what RISE leaves you.** Without Cloud Application Services, you find and request notes; testing and the application's security concept stay yours[28].
- **Own the SIEM rules.** LogServ is optional, and SAP doesn't confirm receipt, write correlation rules or watch alerts[28].
- **Write it into the contract.** Monthly patch status, deadlines for exploited and Critical notes, personal accounts; see the third-party-risk sheet.

What you can skip

- **Buying threat detection first.** Sentinel for SAP or SAP Enterprise Threat Detection sees little while the audit log is off and notes lag.
- **Applying every note on Patch Day.** Support Package Security Notes can wait for the next support package[1].
- **A full SoD rule set first.** Removing SAP_ALL and debug and replace cuts more risk, sooner.

- **RISE transition option.** Security patches from 2031 to 2033, or with further prerequisites to 2035, for systems moved to SAP ERP, private edition on HANA by the end of 2030[27].

What changed in 2026

- **Oracle patches monthly.** Critical Security Patch Updates, first on 28 May, now fill the months between quarterly updates[9].
- **SAP's own npm packages were poisoned.** Malicious CAP database packages and MTA Build Tool versions appeared in April[3]. See the supply-chain sheet.
- **ECC on RISE until 2035.** Since 13 October, the transition option may run to the end of 2035, with further prerequisites[27].

Mistakes that cost the most

- **Leaving unused components installed.** Visual Composer, exploited in 2025, got another 9.9 note in October 2026[4].
- **Falling behind on cumulative patches.** Oracle's fix for CVE-2025-61882 needed the October 2023 Critical Patch Update first[10].
- **Relying on a WAF alone.** Google warns WAF body-inspection rules can be bypassed[8].

What this looks like at your size

Small team, no security staff

- Get a monthly note status per system from your ERP partner, and proof that no ERP login is public.
- In Business Central, limit SUPER and delegated admins[29], and alert on IBAN changes[30].

Growing, with IT or security staff

- Run Patch Day with System Recommendations and track each note into production.
- Move to restrictive gateway files, start UCON logging and alert on emergency user logons.

Enterprise or regulated

- Use SAP Access Control for firefighter IDs, and APP.4.2 or the DSAG guide for audits[12,14].
- Decide by mid-2027 between extended maintenance, the transition option and S/4HANA.

Version history

5 Nov 2026, version 1.0 Published after a copy edit and a source-by-source fact check, which aligned SAP patch deadlines with the patching sheet, added the second exploited Visual Composer flaw, scoped dual control and outbound blocking to what SAP and Google say and marked our trusted RFC rule as an extension of BSI's.

Sources

1. SAP Security Notes & News. SAP, checked 5 Nov 2026. support.sap.com
2. System Recommendations. SAP, checked 5 Nov 2026. support.sap.com
3. SAP Patch Day, April 2026. SAP Support, Apr 2026. support.sap.com
4. SAP Patch Day, October 2026. SAP Support, 13 Oct 2026. support.sap.com
5. Known Exploited Vulnerabilities Catalog. CISA, version 2026.11.04. cisa.gov
6. Microsoft Digital Defense Report 2026. Microsoft Threat Intelligence, Oct 2026. cdn-dynmedia-1.microsoft.com
7. Oracle E-Business Suite Zero-Day Exploited in Widespread Extortion Campaign. Google Cloud, 9 Oct 2025. cloud.google.com
8. ShinyHunters Targets Education Sector with Oracle PeopleSoft Exploit. Google Cloud, 11 Jun 2026. cloud.google.com
9. Critical Patch Updates and Security Alerts. Oracle, Oct 2026. oracle.com
10. Security Alert CVE-2025-61882. Oracle, 6 Oct 2025. oracle.com
11. Critical Security Patch Update, May 2026. Oracle, 28 May 2026. oracle.com
12. APP.4.2 SAP-ERP-System. BSI, Edition 2023. bsi.bund.de
13. APP.4.6 SAP ABAP-Programmierung. BSI, Edition 2023. bsi.bund.de
14. SAP S/4HANA Leitfaden (audit guide). DSAG (user association), Dec 2022. impulsant.dsag.de
15. Ports of SAP NetWeaver AS for ABAP. SAP Help, NW 7.5. help.sap.com
16. Configuring the Gateway Securely. SAP Help, NW 7.5. help.sap.com
17. Using Phase Administration Tools (UCON). SAP Help, NW 7.5. help.sap.com
18. Protecting Special Users. SAP Help, NW 7.5. help.sap.com
19. Monitoring the Emergency Access Session. SAP Learning, checked 5 Nov 2026. learning.sap.com
20. Dual Control for Changing Master Records. SAP Help, SAP ERP, checked 5 Nov 2026. help.sap.com
21. KBA 3404779: Postings for unconfirmed vendors. SAP Support, May 2025. userapps.support.sap.com
22. Setting Up the ABAP Test Cockpit. SAP Help, NW 7.5. help.sap.com
23. SAP Code Vulnerability Analyzer. SAP Community, checked 5 Nov 2026. pages.community.sap.com
24. Sentinel for SAP applications. Microsoft Learn, 13 Aug 2026. learn.microsoft.com
25. Configure SAP for Microsoft Sentinel. Microsoft Learn, 4 Aug 2026. learn.microsoft.com
26. Clarity and Choice on SAP Business Suite 7. SAP, checked 5 Nov 2026. support.sap.com
27. Updates for SAP ERP, Private Edition, Transition Option. SAP News, updated 13 Oct 2026. news.sap.com
28. RISE Roles and Responsibilities, tailored option. SAP, Mar 2026. sap.com
29. Business Central: granular permissions. Microsoft Learn, 3 Mar 2026. learn.microsoft.com
30. Business Central: auditing changes. Microsoft Learn, 17 Jun 2026. learn.microsoft.com