SMB Solutions
CLOUD SERVICES

SMB SOLUTIONS
KNOWLEDGE BASE ARTICLE

Why Staying Current on SAP Business One Matters More Than Ever

Article type	Knowledgebase article
Topic	Keeping SAP Business One, SAP HANA and SUSE Linux up to date
Applies to	SAP Business One 10.0, version for SAP HANA, on SUSE Linux Enterprise Server
Last updated	2 November 2026
Audience	Customers and business owners (non-technical)
Classification	Customer

THE SHORT VERSION

Software flaws are now being found faster than most businesses patch them, and the gap is widening. In October 2026 a serious flaw in the Linux operating system that sits underneath many SAP Business One servers was disclosed, and a working attack was built in a short time with the help of an AI model. Companies running current versions can usually fix a problem like this with a routine update. Companies running old versions may find that no fix exists for them at all.

What just happened

A flaw in the Linux kernel, tracked as CVE-2026-98432, lets a stranger on the network take full control of a server without a password. The kernel is the core of the operating system, the part that handles every incoming connection. The flaw sits in the code that sets up a new internet connection, and it has been there since kernel version 4.4. The Linux kernel team scored it 9.8 out of 10. Some vendors, including SUSE, scored it lower (8.1) because the attack depends on winning a timing race, which is harder to do.

What made this one stand out is how it was found. Anthropic reported that an unreleased AI research model found the bug and then built a working attack on its own. In its test, the model took about 53 minutes to go from the first memory leak to running commands as the all-powerful root user. Anthropic did not publish the attack code.

The fix was ready quickly, but getting it onto servers has been uneven. The Linux developers fixed the flaw in October. As of 30 October, Debian, SUSE, Oracle and Amazon had released fixed kernels for at least some of their products, while Ubuntu and Red Hat had not. SUSE's fixes cover SLES 15 SP4 to SP6 and SLES 16, while SP7 was still waiting for one. There is no fix for older service packs such as SP1, SP2 and SP3. A company running one of those has nothing to install.

© 2026 SMB Solutions. All rights reserved.

Why AI means more of these, not fewer

Finding security flaws used to be slow, specialist work. AI is changing that. Canonical, the company behind Ubuntu, says AI tools have turned bug hunting from a manual, time-intensive process into a highly automated one. It has moved to a new schedule that ships an Ubuntu kernel update every week, because the number of reported flaws has grown so fast.

The Linux flaw is not a one-off. Anthropic's research reported that the same model chained several flaws into working attacks on Chrome, Safari, Android, Windows and Linux. Google assigned 62 CVE identifiers to the Chrome findings alone. Other AI labs report similar results: OpenAI said one of its models found a Firefox flaw during safety testing.

AI is not the only reason the numbers are rising. The Linux kernel team also began assigning CVE identifiers to far more bugs than before. But the direction is clear. Our judgment, not a measured forecast, is that you should plan for a steady stream of new flaws in the operating systems, databases and applications your business runs, and for the time between a flaw being published and an attack appearing to keep shrinking. The same tools that help defenders find bugs are available to attackers.

This does not mean every new CVE is an emergency. Most are lower risk, and many cannot be reached from outside your network. The point is that the volume makes patching a constant job, not an occasional one. A business that updates every few years will always be behind.

Why this matters for SAP Business One

SAP Business One runs on a stack of three layers, and each layer has its own vendor and its own support clock.

Layer	Who supplies it	What happens when it is old
Operating system (SUSE Linux)	SUSE	The vendor stops releasing fixes for old service packs, as with SLES 15 SP1 to SP3 and the Linux flaw above.
Database (SAP HANA)	SAP	Each HANA release has a support end date, and each Business One release lists the HANA revisions it works with.
Business One server components	SAP	SAP stops fixing old releases. Releases 9.0 to 9.3 are already out of mainstream maintenance.

The layers are tied together. Each Business One release lists the operating system versions it supports, and that list moves over time. In SAP's Administrator's Guides, SLES 15 SP2 was removed from the supported list in 10.0 SP 2402, and the SP 2508 guide lists SP4, SP5 and SP6. So a company that stays on an old Business One release is also staying on an old operating system. When that operating system's vendor stops patching it, the company cannot simply patch around the problem. The usual upgrade order is operating system first, then HANA, then Business One, so a late upgrade becomes a multi-step project.

The Business One release itself also has an end date. SAP offers mainstream maintenance only, with no extended maintenance, and releases 9.0 to 9.3 are already out of it. SAP's page has shown different end dates for release 10.0 over time (31 December 2026 in one version, 31 December 2028 in a partner's check dated 22 October 2026), and SAP says dates are subject to change. Confirm the current date directly with SAP.

© 2026 SMB Solutions. All rights reserved.

What falling behind looks like

The Linux flaw shows how it plays out. When it was announced, the fix existed for current releases and for some older ones, but not for others. A company on a current release installed an update and restarted the server. A company on an old release had four bad options:

- **No fix exists.** For the oldest SUSE service packs there is no kernel update to install. The only real fix is to move to a newer release.
- **A fix exists, but only with paid extended support.** SUSE's fixes for the older supported service packs sit in its long-term (LTSS) streams, which need a separate subscription.
- **A temporary workaround.** Admins can block certain network traffic or turn off a feature. These measures only reduce the risk. Even the people publishing them describe them as partial.
- **An emergency upgrade.** The upgrade that was postponed for years now has to happen in days, with little time to test and a business waiting on the system.

There are quieter costs too. SAP Support has told customers that an issue found in 9.3 should be tested in the latest version, and any fix goes into the current release only. And the further behind you are, the harder the jump: when the installed and target releases are more than one version apart, upgrades may need to be done in several steps.

> **An old version that runs well keeps running. That is exactly why the risk is easy to miss. Nothing breaks on the day support ends. The danger is the first time a serious flaw is announced and there is nothing to install.**

What to do now

You do not need to become a security expert. You need to know where you stand and make updating a habit. Your hosting provider usually looks after the servers and operating system, and your Business One partner looks after the application and its upgrades. Ask both.

- ☐ **Write down your versions.** Record your Business One release and patch level, your HANA revision, and your SUSE Linux service pack. Your partner or hosting provider can give you these.
- ☐ **Check each against its support date.** Look up SAP's maintenance page for Business One and SUSE's lifecycle page for your service pack. Note which ones have already ended or end within 18 months.
- ☐ **Ask which of your servers have no fix available** for a flaw like CVE-2026-98432, and whether any of the fixes need paid extended support.
- ☐ **Make updates routine.** Agree a regular maintenance window for operating system updates and restarts, and test each one on a non-production system first.
- ☐ **Plan the next upgrade before you need it.** Book it for a quiet period, with time for testing and user training. The usual order is operating system, then HANA, then Business One.
- ☐ **Limit who can reach your servers.** Keep database and application servers off the open internet, and allow connections only from the systems and people that need them. This reduces your risk in the days between a flaw being published and a fix being installed.

© 2026 SMB Solutions. All rights reserved.

- ☐ **Back up before every change.** Take a HANA backup and a server-level backup before each update, so you can go back if something goes wrong.
- ☐ **Budget for it every year.** Treat upgrades as a regular cost, not a one-off project.

The bottom line

The Linux fix existed within weeks of the flaw being found. Whether a company could use it depended entirely on which version it was running. As AI speeds up the discovery of flaws, that pattern will repeat. Staying current on Business One, HANA and the operating system is the cheapest protection available, because it keeps you in the group that receives fixes.

> **NEED HELP?**
> SMB Solutions looks after your hosting infrastructure. Contact SMB Solutions Support to find out which operating system versions your hosted servers run and whether fixes are available for them. Your SAP Business One support partner looks after the application itself.
>
> **Email:** support@smbsolutions.com.au (creates a support ticket automatically)
> **Australia:** +61 1300 442 059 **New Zealand:** +64 9 974 9196
> **USA:** +1 800 241 3213 **UK / Ireland:** +44 20 3005 2737

Sources

Facts checked 2 November 2026. Vendor status changes quickly, so confirm the current position on each vendor's own page before acting.

- CSO Online: Anthropic AI model finds Linux kernel bug that leads to remote root access
- Aviatrix: CVE-2026-98432 distribution status
- Ostorlab: SUSE fixed kernel versions
- SUSE: CVE-2026-98432 status page
- The Register: CVE flood pushes Ubuntu onto weekly kernel release cycle
- Business Standard: Unreleased Claude model found attack chains in Chrome, Safari
- SAP Business One Administrator's Guide, version for SAP HANA (10.0 SP 2402)
- SAP Business One Administrator's Guide, version for SAP HANA (10.0 SP 2508)
- SAP: Maintenance for SAP Business One

© 2026 SMB Solutions. All rights reserved.