Apple Patches 200+ macOS Security Issues Across Golden Gate 27, Tahoe 26.7 and Sequoia 15.8

TechRounder PDF Edition

Live article:
https://www.techrounder.com/apple/apple-patches-200-macos-security-issues-across-golden-gate-27-tahoe-26-7-and-sequoia-15-8/

By Vipin PG | Published September 15, 2026 | Updated September 15, 2026 | Format: Deep Dive | 10 min read

In brief

Apple’s macOS 27 Golden Gate release arrived with another reason for Mac users to pay attention to the update. The security documentation published alongside it is extensive.

Apple’s macOS 27 Golden Gate release arrived with another reason for Mac users to pay attention to the update. The security documentation published alongside it is extensive.

On September 14, 2026, Apple released macOS 27 Golden Gate, macOS Tahoe 26.7 and macOS Sequoia 15.8. The security advisories for those releases cover more than 200 vulnerability entries, according to 9to5Mac’s review of Apple’s changelogs.

The fixes reach deep into macOS. Apple documents flaws involving arbitrary code execution with kernel privileges, applications gaining root access, sandbox escapes, Gatekeeper bypasses, remote code execution, access to restricted data and modification of protected system files.

There are also fixes involving parts of the Mac that many users rarely think about as security-sensitive, including Bluetooth, printing, WebDAV, SMB file sharing, disk images, archives and Apple Intelligence.

For owners of the final Intel Macs, the release has added significance. Those machines cannot upgrade to macOS 27, which means Tahoe 26.7 is now the current security update for Intel models that remain on Apple’s newest supported Intel operating system.

Apple released three major Mac security updates together

Apple published security documentation for all three macOS releases on September 14.

Update: macOS 27 Golden Gate | Who it is for: Macs supported by Apple’s new macOS generation

Update: macOS Tahoe 26.7 | Who it is for: Macs remaining on Tahoe, including supported Intel Macs

Update: macOS Sequoia 15.8 | Who it is for: Older compatible Macs and systems remaining on Sequoia

Apple’s Golden Gate security advisory alone runs through a long list of operating-system components. Tahoe 26.7 and Sequoia 15.8 contain many of the same CVEs, along with some differences that are specific to those releases.

The 200+ figure needs some context

The figure should not be interpreted as more than 200 separate vulnerabilities affecting every Mac.

Many CVEs appear in two or all three of Apple’s advisories because the same underlying problem exists across multiple macOS generations. Apple lists the fix separately for each affected release.

There are also version-specific entries. Sequoia 15.8, for example, includes an ImageIO vulnerability that Apple says could result in arbitrary code execution when processing an image. That specific entry is not listed in the same form in the Golden Gate advisory.

The size of the combined changelogs still matters, but the type of vulnerability says more about risk than the raw count. Several of the fixes involve some of macOS's strongest security boundaries.

Some flaws could reach kernel privileges

One of the most serious entries in the macOS 27 advisory is CVE-2026-84607 in AVEVideoEncoder.

Apple says a sandboxed application may be able to execute arbitrary code with kernel privileges. The company describes the flaw as a race condition and says it corrected the problem through better state management. Security researcher Ruslan Dautov received credit for reporting it.

The wording matters. Sandboxing normally limits what an application can access, while the kernel operates at the core of the operating system with far greater privileges. A vulnerability capable of moving execution from a sandboxed application to kernel privileges crosses two major security boundaries.

Apple patched another kernel-level code execution issue in the UDF filesystem.

CVE-2026-84506 is a use-after-free vulnerability. According to Apple, an application may be able to execute arbitrary code with kernel privileges. Billy Jheng Bing Jhong and Pan Zhenpeng of STAR Labs SG received credit for the discovery.

A separate UDF vulnerability, CVE-2026-84572, could allow an application to read kernel memory or cause an unexpected system termination.

Several bugs could give an app root access

Root privilege escalation appears repeatedly in Apple's documentation.

The affected components include Bluetooth, CoreServices, CUPS and other parts of macOS. Root access gives software far more control over a Unix-based operating system than an ordinary user-level application normally receives.

In Bluetooth, CVE-2026-84631 could allow an application to gain root privileges. Apple says it fixed the issue by adding entitlement checks.

CoreServices contained another root privilege vulnerability, CVE-2026-43786.

CUPS has multiple privilege-related fixes as well. CVE-2026-43698 and CVE-2026-43691 could allow applications to gain root privileges, while CVE-2026-64790 could allow an app to gain elevated privileges.

That collection of fixes shows why reading beyond the headline vulnerability total is useful. A privilege-escalation flaw can become much more serious when combined with another weakness that provides an attacker with an initial foothold.

Bluetooth includes a remote code execution path

Bluetooth received several fixes in Golden Gate, including CVE-2026-65414.

Apple says a remote attacker may be able to cause an unexpected application termination or execute arbitrary code. The problem was an out-of-bounds write, which Apple addressed through additional bounds checking.

The advisory does not state that simply leaving Bluetooth switched on exposes a Mac to automatic compromise. Apple also does not list CVE-2026-65414 as a vulnerability known to be under active exploitation.

The entry is still notable because Apple explicitly describes the attacker as remote, rather than requiring a malicious application to already be running locally.

macOS printing received several security fixes

CUPS, the printing system used by macOS and other Unix-like operating systems, has one of the more interesting groups of vulnerabilities in the release.

CVE-2026-43692 could allow a remote user to cause an unexpected application termination or arbitrary code execution. Apple says the vulnerability involved insufficient validation and was fixed with better input sanitization.

Aaron Grattafiori of the NVIDIA AI Red Team received credit for the finding.

Other CUPS vulnerabilities have different consequences. CVE-2026-43698 and CVE-2026-43691 could lead to root privileges, while CVE-2026-64790 could provide elevated privileges.

Apple also fixed CUPS issues that could lead to denial-of-service conditions.

Printing is a useful example of the attack surface hidden inside a desktop operating system. The service can interact with applications, files, network devices and remote systems, giving a flaw more security relevance than the familiar print dialog might suggest.

Gatekeeper bypasses appear in several components

Gatekeeper is designed to check downloaded software and help prevent untrusted code from running without the protections macOS normally applies.

Apple’s latest fixes close several paths that could interfere with those checks.

CVE-2026-65399 in copyfile could allow an archive to bypass Gatekeeper. Apple describes it as a file-quarantine bypass.

Another issue in autofs, CVE-2026-84570, could allow an application to bypass Gatekeeper checks. System Settings and WebDAV also received Gatekeeper-related fixes.

WebDAV’s CVE-2026-28899 is especially relevant because WebDAV has other security problems in the same update, including a code execution vulnerability.

Apple closed several sandbox escapes

Application sandboxing is intended to keep an app inside a restricted environment and limit its access to data and system resources.

AppleMobileFileIntegrity contained CVE-2026-65381, which Apple says could allow a malicious application to break out of its sandbox. The issue involved entitlement verification.

Archive Utility has another sandbox escape, CVE-2026-84584, involving symbolic links.

Apple’s advisory also lists sandbox-related vulnerabilities involving Automator, CoreMedia, CoreML, libxpc and macOS quarantine protections.

These fixes are relevant when security bugs are combined. One flaw may get code running, another may remove sandbox restrictions, and a privilege-escalation bug may provide higher system access. Closing each layer makes that type of attack chain harder to build.

A malicious WebDAV server could trigger code execution

WebDAV has one of the clearest network-related code execution entries in Apple’s documentation.

For CVE-2026-65374, Apple says connecting to a malicious WebDAV server may result in code execution. The underlying problem was memory corruption.

The vulnerability was credited to HE WEI and Bruce Dang of Calif.io, with Dang working in collaboration with Claude and Anthropic Research.

Another WebDAV vulnerability, CVE-2026-65375, could cause an unexpected system termination. Apple’s credits again name Bruce Dang, Calif.io, Claude and Anthropic Research.

This category can be particularly relevant in business environments and for users who regularly mount remote storage or connect Macs to network resources outside their direct control.

SMB file sharing has multiple kernel-related fixes

Apple also patched a group of vulnerabilities involving SMB, the network file-sharing protocol commonly used with Windows PCs, NAS devices and file servers.

One vulnerability could allow a malicious SMB share to disclose kernel memory. Another could cause kernel-memory corruption when a Mac connects to a malicious SMB server.

Apple lists other SMB issues capable of causing unexpected system termination or corrupting kernel memory.

These entries do not suggest that ordinary SMB or NAS use becomes unsafe after updating. They show that connecting a computer to an untrusted or compromised file server can expose code inside parts of the operating system that process network filesystems.

Software Update itself had a protected-file flaw

One of the more unusual fixes appears under Software Update.

Apple says CVE-2026-84609 could allow an application to modify protected system files. The permissions problem was fixed through better path validation.

YingMuo of the DEVCORE Research Team received credit for the vulnerability.

Modern macOS versions place strong restrictions around system files. A flaw affecting those protections therefore deserves attention even when an attacker would need another application or access path before reaching it.

Apple Intelligence received a security fix in macOS 27

The Golden Gate advisory also contains a security entry for Apple Intelligence.

CVE-2026-84601 could allow an application to bypass Apple Intelligence security prompts, according to Apple.

Apple describes it as a permissions problem and says improved state management addressed the issue. Nick Cook and Sentry Flag are credited with the finding.

This entry is specific to a part of macOS that is gaining more access to system features and personal context. Permission checks around AI functions are likely to receive more scrutiny as those capabilities become more deeply integrated into the operating system.

Images and other files can still be an attack surface

Several of Apple's fixes involve maliciously crafted content rather than a conventional application.

CoreMedia's CVE-2026-64752, for example, could lead to arbitrary code execution when processing a maliciously crafted image. Apple says it addressed the memory-corruption issue by removing the vulnerable code.

Other entries involve videos, fonts, archives, disk images and additional file formats.

Sequoia 15.8 also contains CVE-2026-65346 in ImageIO. Apple says processing an image may lead to arbitrary code execution. The flaw was an integer overflow and was reported by Nik Tsytsarkin of Meta Red Team X.

The Sequoia entry is a useful reminder that Apple's older supported releases can contain their own fixes rather than receiving a simple copy of the Golden Gate security list.

AI-assisted security research is appearing in Apple's credits

The researcher acknowledgements attached to these releases contain another noteworthy detail.

Apple's macOS 27 documentation names OpenAI Codex Security, the NVIDIA AI Red Team, and researchers working with Claude and Anthropic Research.

OpenAI Codex Security appears in Apple's WebKit acknowledgements alongside Amy Burnett. NVIDIA's AI Red Team is credited on CUPS vulnerabilities, while several entries credit Calif.io researchers working in collaboration with Claude and Anthropic Research.

Those credits do not mean an AI system independently found every vulnerability. Apple frequently credits human researchers, organizations and collaborative research efforts together.

They do provide another concrete example of AI-assisted tools being used in real security research that ends with vulnerabilities reported to a major software vendor and fixed in production releases.

Intel Mac owners have a different upgrade path

macOS 27 Golden Gate drops support for Intel processors.

Apple's macOS 27 security advisory lists MacBook Neo and supported Macs with Apple silicon. Intel Macs are absent from the compatibility list.

Tahoe 26 still supports four Intel Mac families:

- MacBook Pro 16-inch, 2019
- MacBook Pro 13-inch, 2020 with four Thunderbolt 3 ports
- 27-inch iMac, 2020
- Mac Pro, 2019

Those Macs cannot move to Golden Gate. Owners who continue using them should therefore pay close attention to Tahoe 26.7 and future Tahoe security releases.

Sequoia 15.8 remains relevant to older compatible hardware that cannot run Tahoe or to systems intentionally being kept on macOS 15.

Older macOS versions may not receive every security fix

Apple provides a useful warning in its software-update documentation.

The company says dependencies on architecture and system changes can mean that not all known security issues are addressed in previous operating-system versions.

That means receiving a Tahoe or Sequoia security update does not guarantee that an older release contains every security change present in macOS 27.

This does not make Tahoe 26.7 or Sequoia 15.8 unsafe. Both have received extensive fixes in this release. Users who cannot upgrade to Golden Gate should still install the newest update offered for their Mac.

For Macs that do support macOS 27, security coverage is one factor to consider alongside software compatibility and stability when deciding when to move to the new operating system.

Apple has not listed these flaws as actively exploited

The severity of some entries can make terms such as "kernel code execution" and "remote code execution" sound like confirmation of an ongoing attack campaign. Apple’s published advisories do not currently say that.

As of September 15, Apple’s security pages for macOS 27 Golden Gate, Tahoe 26.7 and Sequoia 15.8 do not contain Apple’s usual language stating that it is aware of a vulnerability being exploited in the wild.

There is also no basis in the published advisories for referring to the entire group as zero-day vulnerabilities.

The impact descriptions explain what exploitation could allow under the required conditions. They should not be read as evidence that every unpatched Mac is already being attacked through these flaws.

Which update should Mac users install?

The right version depends on the Mac and the operating system you plan to keep using.

- Macs ready for Golden Gate: macOS 27 includes the fixes documented for Apple’s new operating-system generation.
- Macs staying on Tahoe: install macOS 26.7 rather than remaining on an earlier Tahoe release.
- Intel Macs supported by Tahoe: macOS 26.7 is the current path because those machines cannot install macOS 27.
- Macs remaining on Sequoia: install macOS 15.8 to receive the fixes Apple has provided for that release.

A major operating-system upgrade can require more planning than a point update, especially on a Mac used for work or with software that has strict compatibility requirements. A current backup is sensible before making the move.

If you use a Mac, I recommend checking System Settings > General > Software Update and installing the newest security update that fits your hardware and macOS version once your backup and application compatibility are in order.