Apple Security Bounty Guidelines

Submit your research

Submit your report online to help ensure that you receive timely updates, can add additional information as needed, and can communicate with Apple security engineers about your report. Visit Apple Security Research, click Submit a Report, and sign in to your Apple Account.

Apple prioritizes complete and actionable reports that let us quickly investigate, confirm, and address security issues — and that help you qualify for Apple Security Bounty rewards.

Report criteria

A complete and actionable report includes:

- ***A precise, clear explanation of the issue, with concise descriptions*** of the behavior you observed, the behavior you expected, the security or privacy mechanism that was bypassed, and an explanation of how it might be exploited by an attacker. Avoid lengthy descriptions generated by AI tools.
- A **working exploit** that explains the conditions required to start the attack and the control, data, or privilege you gain by the end of the attack — or a reliable **proof of concept (PoC)** for the issue you're reporting. Your report must at least include a concise, numbered list of steps required to reproduce the issue.
- Use of **Target Flags**, if applicable. For example, to demonstrate kernel-level privilege escalation, your report needs to include proof that you obtained our target flag in the commpage. You still need to include a PoC that demonstrates you accessed the target flag through privilege escalation. Target Flags are not available for all categories and reward levels within a given category.

To see the most up-to-date list of research areas that require use of Target Flags to be eligible for the stated reward, visit the Categories page. If Target Flags are not available for your research category, you must still provide the other requirements for a complete and actionable report.

Best practices

- Reports of zero-click or one-click vulnerabilities — or any issue that requires execution of multiple exploits — must include a full chain to receive the stated reward. Submit such issues as a single report with both compiled and source versions, a sample nondestructive payload (if needed) and everything required to execute the chain.
- Include your exploit or PoC as an attachment. If you provide an exploit chain, please create a password-protected archive and attach it to your report. Avoid attaching a link to a web-hosted PoC or video.
- For issues such as UI authentication or Lock Screen bypass reports, provide a high-quality video demonstration. Use the built-in screen recorder for Mac, iPhone, and iPad whenever possible.
- Include the crash log for issues that cause a process to crash. For other issues, capture a sysdiagnose with the most applicable profile installed on your device and note the timestamp when you reproduced the issue.

Reward eligibility

Only the first complete and actionable report we receive for an issue is eligible for a reward, even if it's not the first or only report we receive.

To be eligible for Apple Security Bounty rewards:

- You must be the first party to submit a complete and actionable report directly to Apple through our web portal.
- The report must be of an exploitable security bug that would result in the potential for real-world threat to users.
- Your report must include a reliable way to reproduce the issue.
- The issue must not be publicly disclosed before Apple releases an update with a security advisory for the report.
- For Product categories, the issue must affect the latest publicly available version (including beta versions) of iOS, iPadOS, macOS, tvOS, visionOS, or watchOS, with a standard configuration and on publicly available Apple hardware or Security Research Device.
- For Services, the issue must relate to a web server or service owned by Apple or an Apple subsidiary.

Issues of low impact to real-world user security that we address with a software fix out of an abundance of caution may be eligible for a $1,000 bounty reward, in addition to crediting the researcher and assigning a CVE-ID.

To be eligible for the **stated** Apple Security Bounty rewards:

- The issue must affect the latest publicly available software and hardware with standard configurations, including Apple-designed components — Apple silicon, cellular modems, and networking chips — where relevant.
- You must submit a complete and actionable report, as described above, which includes a working exploit that demonstrates how the issue might be used to target the system, and confirmation with Target Flags, if applicable.

Some issues may be eligible for an additional bonus. For example, security issues that are unique to newly added features or code in developer or public beta software — including newly introduced regressions — may qualify for a 50 percent bonus, if they're reported before the beta period ends. Reports that successfully bypass the specific protections of Lockdown Mode may qualify for a 100 percent bonus. Please note that Private Cloud Compute (PCC) server software does not have beta releases, and Lockdown Mode does not apply to PCC.

Example rewards are published on the Apple Security Bounty Categories page.

What to expect

Apple reviews all reports that you submit directly to us. When you submit your research on the web, you'll receive an immediate automatic acknowledgement that we received your report. You can sign in to your Apple Account at the Apple Security Research site to see the status of your report.

Apple updates your report status when we review it, when we make a determination about its impact, and — for eligible issues — when it's addressed. If we need additional information, we'll add a comment to your report and notify you using the email address associated with your Apple Account. If you have any questions, or want to provide more information to help us reproduce or investigate an issue, you can add comments or attachments to your report at any time. We make it a priority to resolve security and privacy issues as quickly as possible, and most reports are resolved within 90 days.

Apple Security Bounty rewards

If your report qualifies for a reward, the report page displays more information, including bounty status, amount, and next steps. We consider any issue with security impact to users for a potential reward, even if it doesn't match the Apple Security Bounty Categories description.

For the protection of our users, Apple doesn't publicly disclose security issues until our investigation is complete and any necessary updates are generally available. **Publicly disclosing security issues before a fix is available makes you ineligible for all Apple Security Bounty rewards**.

Accelerated awards with Target Flags

Target Flags help us review security research more quickly, so reports submitted using Target Flags qualify for accelerated awards, which we process even before a fix becomes available. After an Apple engineer confirms your report, we notify you of your reward, but you must still refrain from disclosing the issue until we release a fix to remain eligible for rewards.

Evaluating full exploit chains

We give you additional time to create and submit complex exploit chains. After you demonstrate security impact for part of a chain — by capturing the appropriate Target Flag or otherwise — you may submit this work for a reward immediately, even before you demonstrate a chained attack. You may then submit a new report with the complete chain and as long as you do so before we release the relevant security update, we'll reassess your report with the additional chain research for a potentially higher reward. Add a comment to your original report to notify us of your new report.

Requesting Reassessment

With the exception of reports that successfully make use of Target Flags, we make Apple Security Bounty reward decisions **after** resolving the security issue to ensure comprehensive assessment of your report. If you believe we missed important information that you already provided, you can request a reassessment within three weeks of our reward decision by replying to your original report.

We will not reassess reports with new information added after the issue is resolved, with the exception of exploit chains that demonstrate a chained attack.

Apple Security Bounty rewards change over time based on our security and privacy goals. Past rewards are not a guarantee of future rewards.

Apple security advisories

Researchers who report new security or privacy vulnerabilities in Apple platforms are eligible for public acknowledgement in security advisories that accompany software releases. We typically credit researchers as follows: “Jane Appleseed of Security Research Company.” If you notice an error in your credited name, you may request a correction within 30 days of publication through your original report. Acknowledgements that contain inappropriate, offensive, or other unprofessional content are not published.

If you prefer not to be publicly acknowledged for your finding, let us know in your report. In such cases, we credit “an anonymous researcher” to maintain transparency related to security issues that were externally disclosed to us.

Donate a reward

Apple doubles rewards when donated to qualifying causes. If you’d like your reward amount to be donated, request more information by replying to your official Apple Security Bounty notification.

Ineligible Reports

Before you submit your report, validate your research and confirm that it meets all our requirements. Certain reports are ineligible for Apple Security Bounty rewards, including:

- Reports that are incomplete or not actionable, even if you were the first to report — such as reports without a reliable way to reproduce the issue.
- Infeasible reports, such as reports of theoretical issues or issues discovered by AI without proper validation.
- Brute force attacks to achieve access to Target Flags.
- Reports about third-party hardware, software, or services, which should be reported to the developer or manufacturer.
- Other reports that we deem ineligible. See Apple Security Bounty Terms and Conditions for details.

Repeated submissions of ineligible reports

If you repeatedly submit ineligible reports — including infeasible reports about theoretical issues or those discovered by AI without proper validation — we may pause processing your reports for 180 days. Researchers with more than two paused status periods may be permanently removed from the Apple Security Bounty program.

We receive many reports claiming to be about serious security or privacy issues, but that are generated by LLMs and submitted without the required proof or validation by a person. Investigating these and other ineligible reports can prevent us from acting quickly to resolve serious and critical security issues.

If your status in Apple Security Bounty is paused, you are ineligible for bounty rewards or credit in security advisories during this time. We will not process your reports, unless your report clearly demonstrates the security or privacy issue by capturing the applicable Target Flag or with a fully packaged virtualization of iOS or macOS.

Apple Security Bounty Categories

Learn more ›

Terms and Conditions

Learn more ›

* Reports are eligible whether Lockdown Mode is enabled or disabled.

Copyright © 2026 Apple Inc. All rights reserved.