How Google handles security vulnerabilities

As a provider of products and services for many users across the internet, we recognize how important it is to help protect user privacy and security. We understand that secure products are instrumental in maintaining the trust users place in us and we strive to create innovative products that both serve user needs and operate in the user's best interest.

This site provides information for developers and security professionals.

If you are a Google user and have a security issue to report regarding your personal Google account, please visit our contact page. To find out how to stay safe online, take the Google Security Checkup.

Reporting security issues

If you believe you have discovered a vulnerability in a Google product or have a security incident to report, go to bughunters.google.com/report to include it in our Vulnerability Reward Program. Upon receipt of your message we will send an automated reply that includes a tracking identifier. If you feel the need, please use our PGP public key to encrypt your communications with us.

On request, we will issue CVEs for any valid vulnerabilities that are within scope of Google CNAs. In addition, we will publish all CVE-related details in accordance with the other commitments made to the public disclosure timeline on this page.

Google's vulnerability disclosure policy

why Google adheres to a 90-day disclosure deadline. We notify vendors of vulnerabilities immediately, with details shared in public with the defensive community after 90 days, or sooner if the vendor releases a fix. That deadline can vary in the following ways:

- If a deadline is due to expire on a weekend or US public holiday, the deadline will be moved to the next normal work day.
- Before the 90-day deadline has expired, if a vendor lets us know that a patch is scheduled for release on a specific day that will fall within 14 days following the deadline, we will delay the public disclosure until the availability of the patch.
- When we observe a previously unknown and unpatched vulnerability in software under active exploitation (a “0day”), we believe that more urgent action—within 7 days—is appropriate. The reason for this special designation is that each day an actively exploited vulnerability remains undisclosed to the public and unpatched, more devices or accounts will be compromised. Seven days is an aggressive timeline and may be too short for some vendors to update their products, but it should be enough time to publish advice about possible mitigations, such as temporarily disabling a service, restricting access, or contacting the vendor for more information. As a result, after 7 days have elapsed without a patch or advisory, we will support researchers making details available so that users can take steps to protect themselves. We believe it’s important that vendors disclose that there is evidence to suggest that the vulnerability is under active exploitation. Google does this through a product’s security bulletin.

As always, we reserve the right to bring deadlines forwards or backwards based on extreme circumstances. We remain committed to treating all vendors strictly equally. Google expects to be held to the same standard.

This policy is strongly in line with our desire to improve industry response times to security bugs, but also results in softer landings for bugs marginally over deadline. We call on all reasoning compelling. Creating pressure towards more reasonably-timed fixes will result in smaller windows of opportunity for blackhats to abuse vulnerabilities. In our opinion, vulnerability disclosure policies such as ours result in greater overall safety for users of the Internet.

Resources

Blog

Brand Resource Center

Careers

Contact us

Help Center

Investor Relations

Locations

Press resources

Outreach and initiatives

Accessibility

Crisis Response

Google.org

Google for Health

Grow with Google

Learning

Public Policy

Sustainability

Research and technology

Google AI

Google Cloud

Google DeepMind

Google for Developers

Google Labs

Google Research

More about us

Human rights

Safety Center

Supplier responsibility

Transparency Center

Transparency Report

Google Privacy Terms

? Help English