Google Security Blog

The latest news and insights from Google on security and safety on the Internet

Feedback and data-driven updates to Google's disclosure policy

February 13, 2015

Posted by Chris Evans and Ben Hawkes, Project Zero; Heather Adkins, Matt Moore and Michal Zalewski, Google Security; Gerhard Eschelbeck, Vice President, Google Security

Cross-posted from the Project Zero blog

Disclosure deadlines have long been an industry standard practice. They improve end-user security by getting security patches to users faster. As noted in CERT's 45-day disclosure policy, they also "balance the need of the public to be informed of security vulnerabilities with vendors' need for time to respond effectively". Yahoo!'s 90-day policy notes that "Time is of the essence when we discover these types of issues: the more quickly we address the risks, the less harm an attack can cause". ZDI's 120-day policy notes that releasing vulnerability details can "enable the defensive community to protect the user".

Deadlines also acknowledge an uncomfortable fact that is alluded to by some of the above policies: the offensive security community invests considerably more into vulnerability research than the defensive community. Therefore, when we find a vulnerability in a high profile target, it is often already known by advanced and stealthy actors.

Project Zero has adhered to a 90-day disclosure deadline. Now we are applying this approach for the rest of Google as well. 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. We've chosen a middle-of-the-road deadline timeline and feel it's reasonably calibrated for the current state of the industry.

To see how things are going, we crunched some data on Project Zero's disclosures to date. For example, the Adobe Flash team probably has the largest install base and number of build combinations of any of the products we've researched so far. To date, they have fixed 37 Project Zero vulnerabilities (or 100%) within the 90-day deadline. More generally, of 154 Project Zero bugs fixed so far, 85% were fixed within 90 days. Restrict this to the 73 issues filed and fixed after Oct 1st, 2014, and 95% were fixed within 90 days. Furthermore, recent well-discussed deadline misses were typically fixed very quickly after 90 days. Looking ahead, we're not going to have any deadline misses for at least the rest of February.

Deadlines appear to be working to improve patch times and end user security—especially when enforced consistently.

We've studied the above data and taken on board some great debate and external feedback around some of the corner cases for disclosure deadlines. We have improved the policy in the following ways:

- **Weekends and holidays.** 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.
- **Grace period.** We now have a 14-day grace period. If a 90-day deadline will expire but a vendor lets us know before the deadline that a patch is scheduled for release on a specific day within 14 days following the deadline, the public disclosure will be delayed until the availability of the patch. Public disclosure of an unpatched issue now only occurs if a deadline will be significantly missed (2 weeks+).

- **Assignment of CVEs.** CVEs are an industry standard for uniquely identifying vulnerabilities. To avoid confusion, it's important that the first public mention of a vulnerability should include a CVE. For vulnerabilities that go past deadline, we'll ensure that a CVE has been pre-assigned.

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; in fact, Project Zero has bugs in the pipeline for Google products (Chrome and Android) and these are subject to the same deadline policy.

Putting everything together, we believe the policy updates are still strongly in line with our desire to improve industry response times to security bugs, but will result in softer landings for bugs marginally over deadline. Finally, we'd like to call on all researchers to adopt disclosure deadlines in some form, and feel free to use our policy verbatim if you find our data and reasoning compelling. We're excited by the early results that disclosure deadlines are delivering—and with the help of the broader community, we can achieve even more.

No comments :

Post a Comment