Google Security Blog

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

Disclosure timeline for vulnerabilities under active attack

May 29, 2013

Posted by Chris Evans and Drew Hintz, Security Engineers

We recently discovered that attackers are actively targeting a previously unknown and unpatched vulnerability in software belonging to another company. This isn't an isolated incident -- on a semi-regular basis, Google security researchers uncover real-world exploitation of publicly unknown ("zero-day") vulnerabilities. We always report these cases to the affected vendor immediately, and we work closely with them to drive the issue to resolution. Over the years, we've reported dozens of actively exploited zero-day vulnerabilities to affected vendors, including XML parsing vulnerabilities, universal cross-site scripting bugs, and targeted web application attacks.

Often, we find that zero-day vulnerabilities are used to target a limited subset of people. In many cases, this targeting actually makes the attack more serious than a broader attack, and more urgent to resolve quickly. Political activists are frequent targets, and the consequences of being compromised can have real safety implications in parts of the world.

Our standing recommendation is that companies should fix critical vulnerabilities within 60 days -- or, if a fix is not possible, they should notify the public about the risk and offer workarounds. We encourage researchers to publish their findings if

reported issues will take longer to patch. Based on our experience, however, we believe that more urgent action -- within 7 days -- is appropriate for critical vulnerabilities under active exploitation. The reason for this special designation is that each day an actively exploited vulnerability remains undisclosed to the public and unpatched, more computers 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. By holding ourselves to the same standard, we hope to improve both the state of web security and the coordination of vulnerability management.

8 comments :

Unknown said...

Incredible that this is still debated at all! If you have wide spread software and there is a critical security hole: You fix it! NAO!

7 days is nice as a start. But actually bits and bytes know speed a little different than us puny humans. 7 days is enough to infect the whole world!

May 30, 2013 at 6:02 AM

chillzwerg said...

Better and faster security. Superb!

May 30, 2013 at 11:14 AM

voodooKobra said...

I approve of this maneuver. If the vendor doesn't respond after a week, they cannot be trusted to secure their customers.

May 30, 2013 at 2:41 PM

killbit said...

This is a fantastic policy for companies that are cloud based such as good. However those companies that provide enterprise software a customer has to install and test. is NOT going to be able to fix, test, release to customer, customer pick up the fix, customer test, submit change

requests and deploy in < 7 days. You guys are going to expose more customers to these sorts of issues. Why not work with the companies to release guidance if they can't fix the issue. Google has no idea about enterprise customers. No enterprise is going to pick up any software from you they have to deploy.

May 30, 2013 at 4:15 PM

Unknown said...

I like it. Way to keep us safe :-D

May 30, 2013 at 4:37 PM

Anonymous said...

Will you also be holding the rest of Google to the same standard?

May 31, 2013 at 9:36 AM

007 said...

Approved !

May 31, 2013 at 11:01 AM

Joe Philipps said...

Compared to some researchers, this is charitable. A certain proportion of them think full disclosure should be the norm so that the affected parties can begin to mitigate the trouble.

May 31, 2013 at 3:27 PM

Post a Comment