Improving Security for Bugzilla

Frequently asked questions

What happened?

Bugzilla restricts access to security-sensitive information so that only certain privileged users can access it. An attacker was able to break into a privileged user's account and download security-sensitive information about flaws in Firefox and other Mozilla products.

How did the attacker gain access?

The attacker acquired the password of a privileged Bugzilla user, who had access to security-sensitive information. Information uncovered in our investigation suggests that the user re-used their Bugzilla password with another website, and the password was revealed through a data breach at that site.

How long did the attacker have access?

The earliest confirmed instance of unauthorized access dates to September 2014. There are some indications that the attacker may have had access since September 2013.

What immediate actions has Mozilla taken?

Upon discovery of the unauthorized access, Mozilla's security team shut down the compromised account and began to assess the scope of the information that was available to the attacker. We conducted audits of several other systems to look for other evidence of compromise. We also worked with an outside security firm to conduct forensic analysis.

What else has Mozilla done to prevent it happening in the future?

We are taking several steps to be more restrictive in who can have access to security-sensitive information in Bugzilla and how they can access it. First, we are making it harder to break into Bugzilla accounts. Passwords have been reset for all privileged users, and going forward, all privileged users will be required to use two-factor authentication to log into Bugzilla. Second, we are reducing the access that each Bugzilla user is granted in order to limit the amount of information that could potentially be exposed in the event of unauthorized access. Third, we are increasing the amount of auditing we do on the actions of privileged users so that we can detect suspicious activity more quickly and accurately.

What security information did the attacker have access to?

Bugzilla tracks information in units of “bugs”. Each “bug” in Bugzilla typically represents a single flaw to be fixed, or a single improvement to be made. Bugzilla’s logs allow us to see exactly which bugs the attacker accessed and when.

Overall, the attacker accessed 185 non-public bugs, distributed as follows:

110 bugs	Protected for reasons other than software security (e.g., proprietary information)
22 bugs	Minor security issues (sec-low or sec-moderate)
53 bugs	Severe vulnerabilities (sec-high or sec-critical)

Of these 53 sec-high or sec-critical bugs, 43 had already been fixed in the released version of Firefox at the time the attacker found out about them. The information in those bugs likely could not have been used to attack Firefox users.

For the remaining 10 bugs, the attacker had some window of time between when the bug was accessed and when it was fixed in Firefox:

2 bugs	Less than 7 days
5 bugs	Between 7 days and 36 days
3 bugs	More than 36 days (131 days, 157 days, 335 days)

It is technically possible that any of these bugs could have been used to attack Firefox users in the vulnerability window. One of the bugs open less than 36 days was used for an attack using a vulnerability that was patched on August 6, 2015. Other than that attack, however, we do not have any data indicating that other bugs were exploited.

What impact has this had on Firefox users?

The largest known impact on users is through the vulnerability we fixed on August 6th. We know that an attack exploiting that vulnerability was used to collect private data from Firefox users visiting a news site in Russia. There is no indication that any of the other bugs the attacker accessed have been exploited.

How can Firefox users protect themselves?

The best way for users to protect themselves is to run the latest version of Firefox. On August 27, we released new versions of desktop Firefox, Firefox for Android, and Firefox ESR. These versions address fixes all of the vulnerabilities that the attacker learned about and could have used to harm Firefox users.