01 Aug 2012 (SA-WEB-2012-007)

Submitted	01 August 2012
Advisory ID	SA-WEB-2012-007
Risk	Highly critical
Platform	Ushahidi

Description:

The following security issues are fixed in 2.5 thanks to help from OWASP Portland:

Multiple SQL injections. Discovered by postmodern, Kees Cook and Timothy D. Morgan.
Multiple SQL injections have been found and the queries fixed.

CVE-2012-3468 - issues discovered by Ushahidi dev team
CVE-2012-3469 - issues discovered by postmodern
CVE-2012-3470 - issues discovered by Kees Cook
CVE-2012-3471 - issues discovered by Timothy D. Morgan

Missing authentication on comments and reports API calls. Discovered by Kees Cook. (CVE-2012-3473)
The comments API was missing authentication on comment actions (ie. approve/unapprove/spam) and on listing comments usually only available to admins. Authentication is now required.

Missing authentication on email API calls. Discovered by Dennison Williams. (CVE-2012-3472)
The email API exposes sensitive information usually only available to an admin. However API requests were not being authenticated. The API now requires admin authentication.

Admin user hijacking through the installer. Discovered by Wil Clouser. (CVE-2012-3475)
Ushahidi's installer allows users to create an admin user during install. However requests after install were not being properly redirected and could be hijacked. Users are recommended to delete the installer directory after installer.

Stored XSS on member profile pages. Discovered by Amy K. Farrell (CVE-2012-3476)
Some data displayed on member profile pages was not being properly escaped. This is mitigated by Kohana's automatic XSS cleaning of input but could still be
exploited with sufficient effort.

User data exposed in comments API. Discovered by the Ushahidi dev team (CVE-2012-3474)
Comments email and ip address were being exposed in the comments API without authentication. This information has been removed.

Instructions:

This vulnerability can be fixed by upgrading to 2.5. An upgrade to our latest version is highly recommended.

For users who cannot upgrade (ie. if you are running an early Ushahidi version) you can patch your install with the patch attached to this post:

- Download and unzip patch_2.4_2012_007 (below).
- Upload and replace your current files in the folders that correspond to those in the patch.

Download (ZIP; click to download)	md5
Patch patch_2.4_2012_007 for v2.4.1 and earlier	