Main page
Recent changes
Server admin log (Prod)
Server admin log (RelEng)
Deployments
SRE/Operations Help
Incident status

Cloud VPS & Toolforge
Cloud VPS documentation
Toolforge documentation
Request Cloud VPS project
Server admin log (Cloud VPS)

Tools
What links here
Related changes
Special pages
Permanent link
Page information
Cite this page

Print/export
Create a book
Download as PDF
Printable version

Incident documentation/20150820-PageCategorization (Privacy)

< Incident documentation

Contents [hide]

Summary

Between Aug 18th and Aug 20th, a patch was deployed to some wikis (group0 and group1 deployment groups) on the WMF cluster that caused MediaWiki to report IP addresses of editors who cause a category to be added to a page under certain conditions. When the category was added as part of a parser function triggered from a subsequent call to the purge API, the recent changes log reported the IP address from which the purge originated, even when called by a logged in editor. The proximity in the recent changes log of these changes to other edits could have allowed an observer to associate the IP address and username of an editor. The publication of this combination of data is considered a violation of our privacy policy.

Once the issue was confirmed and problem patch identified, the Security team immediately began the process of reverting the feature, and deleting all recent changes entries created by the patch to prevent leaking this private data further.

During the time that the patch was deployed, the API call that could have triggered this leak of private information was called 340 times (326 times on commons.wikimedia.org, 10 times on pl.wiktionary.org, and 4 times on en.wiktionary.org) by 69 different IP addresses.

Timeline

- 2015-08-18 18:30 UTC: 1.26wmf19 (which contained Gerrit 211526) was deployed to group0 wikis (testwiki, test2wiki, mediawikiwiki, zerowiki, testwikidatawiki)
- 2015-08-19 18:06 UTC: 1.26wmf19 deployed to group1 wikis (non-Wikipedia wikis)
- 2015-08-19 21:49 UTC: User Peter Bowman reports bug T109638
- Approximately 2015-08-20 18:00 UTC: Release Engineering deploys revert (Gerrit 232764)
- 2015-08-20 20:25 UTC: Script to delete recentchanges rows finishes

Conclusions

The patch that caused the issue was created, reviewed, and merged by experienced staff and volunteer developers, yet each of these developers failed to identify the potential security impact of the design. This indicates that the security ramifications of the functions involved are likely not structured or documented in a way that makes the issues clear, and this particular code pattern has not been highlighted as dangerous in documentation or training. Additionally, there are currently no automated or manual testing procedures specifically to identify privacy issues in new version of MediaWiki.

Actionables

In the near term, we will add notice about User::newFromId(0) to secure code training (bug T110620), and investigate updating the function definition or documentation to make the security impact more clear to developers.

Longer term, we will investigate using static analysis tools to automatically flag this code pattern (depends on bug T110617, and look at developing security training specifically for QA testers, which would include looking for

privacy issues.

Category: Incident documentation