RISK ASSESSMENT —

Researchers find “severe” flaw in WordPress plugin with 1 million installs

If you use NextGEN Gallery, now would be a good time to update.

DAN GOODIN - 2/28/2017, 11:13 AM

More than 1 million websites running the WordPress content management system may be vulnerable to hacks that allow visitors to snatch password data and secret keys out of databases, at least under certain conditions.

The vulnerability stems from a "severe" SQL injection bug in NextGEN Gallery, a WordPress plugin with more than 1 million installations. Until the flaw was recently fixed, NextGEN Gallery allowed input from untrusted visitors to be included in WordPress-prepared SQL queries. Under certain conditions, attackers can exploit the weakness to pipe powerful commands to a Web server's backend database.

"This is quite a critical issue," Slavco Mihajloski, a researcher with Web security firm Sucuri, wrote in a blog post published Monday. "If you're using a vulnerable version of this plugin, update as soon as possible."

To exploit the vulnerability, attackers would have to create a feature found in the PHP programming language known as the $container_ids string. Untrusted visitors could achieve this against sites that use the NextGEN Basic TagCloud gallery feature by making slight modifications to the gallery URL.

"With this knowledge, an unauthenticated attacker could add extra sprintf/printf directives to the SQL query and use $wpdb->prepare's behavior to add attacker controlled code to the executed query," Monday's blog post explained.

For the attack to work, a website would have to be set up to allow users to submit posts to be reviewed. An attacker could create an account on the site and submit a post that contains malformed NextGEN Gallery shortcodes.

Mihajloski also described a scenario under which privileged authenticated users could perform the attack.

Sucuri has assigned a severity rating of 9 out of a possible 10 points to the vulnerability, which was fixed in version 2.1.79 of the plugin. The update changelog makes no reference to the vulnerability, so

it's not clear how widely known the threat is. As Sucuri notes, website administrators who rely on NextGEN Gallery should install the fix immediately.

Promoted Comments

rflnogueira / Smack-Fu Master, in training JUMP TO POST

It may be a plugin issue, but it's the platform's role to prevent any plugin from doing this kind of damage. There is no excuse for SQL injections in 2017, other than sloppy development and bad architecture decisions.

From my perpective (software developer), having worked with different CMSs over a few years, I think it's full of architectural awkwardnesses, code smells, security breaches waiting to hatch and laziness on testing. It's very ugly PHP.

In the rare instances it worked well, the system was so heavily modified the company could have created a new CMS with that kind of budget.

7 posts | registered 12/19/2012

DAN GOODIN
Dan is the Security Editor at Ars Technica, which he joined in 2012 after working for The Register, the Associated Press, Bloomberg News, and other publications.

EMAIL dan.goodin@arstechnica.com // **TWITTER** @dangoodin001

READER COMMENTS 74 SHARE THIS STORY

← PREVIOUS STORY NEXT STORY →

Related Stories

Today on Ars