

Hash Suite - Windows password security audit tool. GUI, reports in PDF.

[<prev] [next>] [day] [month] [year] [list]

Date: Wed, 19 Feb 2020 09:03:04 +0100

From: Hanno Böck <hanno@hboeck.de>

To: oss-security@lists.openwall.com

Subject: Wordpress themegrill-demo-importer: database reset/auth bypass,
incomplete fix due to CSRF

A severe vulnerability in a wordpress plugin called ThemeGrill Demo
Importer was discovered by the company WebARX:
<https://www.webarxsecurity.com/critical-issue-in-themegrill-demo-importer/>

The vulnerability is as follows:

The plugin adds a hook to wordpress that can be reached with the
ajax-interface (admin-ajax.php) and that has a functionality to reset
the wordpress database which will be triggered if the GET variable
do_reset_wordpress is set.

The problem: This had no authentication whatsoever.

PoC:
curl https://example.org/wp-admin/admin-ajax.php?do_reset_wordpress01
--data 'action=heartbeat' -i

This can obviously delete all existing posts and other data. If there
exists a user called "admin" (i.e. the name of the user is admin, not
just a user with an admin role) then after triggering that function the
attacking user will be logged in as the admin, so in that case he can
use that to e.g. install a plugin and gain code execution. For further
details read the WebARX post.

This is already being actively exploited, I observed several vulnerable
installations that were empty yesterday (i.e. only showing the standard
"Hello World" post of a new wordpress installation).

Incomplete Fix / CSRF
=====

As a fix for this the developers of the plugin added a check if one is
logged in as a user with sufficient permission in version 1.6.2.
This is not a full fix, because there is no protection from Cross Site
Request Forgery. This means the functionality can no longer be
triggered by an unauthenticated user, but one can lure the admin of an
affected site to a site triggering a POST request executing that
function.

PoC code:
<form id="f1"
action="https://example.org/wp-admin/admin-ajax.php?do_reset_wordpress=1"
method="POST"> <input type="hidden" name="action" value="heartbeat">
</form>
<script>
document.getElementById("f1").submit();
</script>

I had reported this to the developers of the plugin on Monday, but
given that this is almost entirely obvious looking at the fix I was
likely not the only one who has noticed. WebARX also told me they
noticed this and had already told Themegrill about it.

There's now an update 1.6.3 that adds a nonce check. I have
not reviewed that change in detail. Patches:
<https://github.com/themegrill/themegrill-demo-importer/commit/b350a29628fb40522468a576e98e45abbc4de0c7>
<https://github.com/themegrill/themegrill-demo-importer/commit/564d8496d1f0d10f6aab4798eeec7ddefc81bdd2>

From the functionality this plugin provides I believe it's only useful
during development and testing of themes. Therefore even if the
vulnerability is now hopefully fixed it is probably a good idea to
remove it from production installations when it's no longer needed.

Summary on affected versions:
1.3.4 to 1.6.1: vulnerable to original/severe variant
1.6.2: Insufficient fix, attack with CSRF possible
1.6.3: hopefully fixed

--
Hanno Böck
<https://hboeck.de/>

Powered by blists - more mailing lists

Please check out the [Open Source Software Security Wiki](#), which is counterpart to this [mailing list](#).

Confused about [mailing lists](#) and their use? [Read about mailing lists on Wikipedia](#) and check out these [guidelines on proper formatting of your messages](#).

