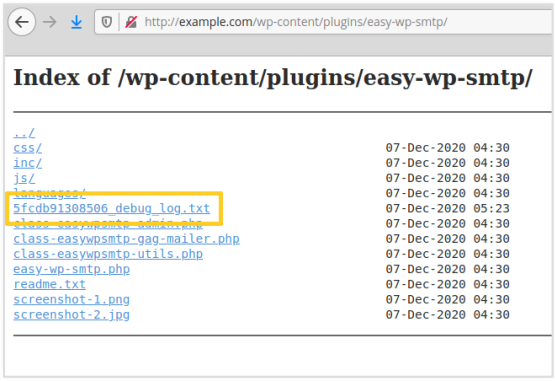
WordPress Easy WP SMTP plugin fixed zero-day vulnerability.

BY JEROME BRUANDET DECEMBER 7, 2020 - 1:28PM [+0700]

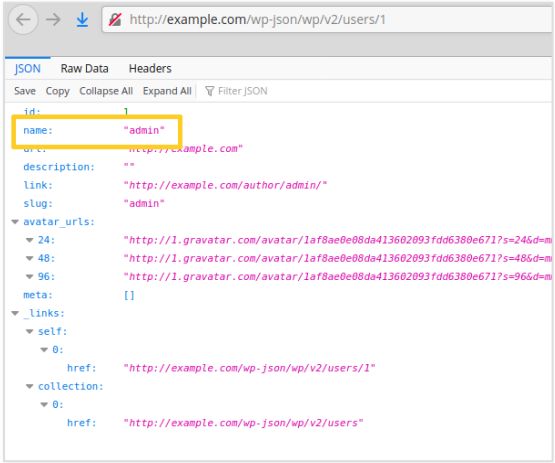
The WordPress Easy WP SMTP plugin, which has 500,000+ active installations, fixed a zero-day vulnerability affecting version 1.4.2 and below that could allow an unauthenticated user to reset the admin password among other issues.

> This vulnerability is currently exploited, make sure to update as soon as possible to the latest version.

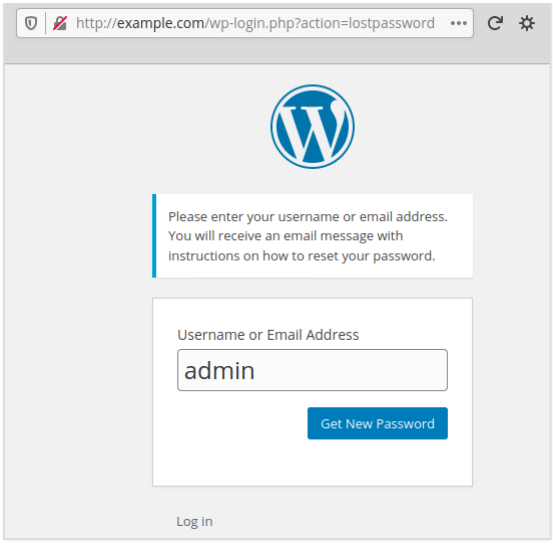
The Easy WP SMTP plugin has an optional debug log where it writes all email messages (headers and body) sent by the blog. It is located inside the plugin's installation folder, "/wp-content/plugins/easy-wp-smtp/". The log is a text file with a random name, e.g., 5fcdb91308506_debug_log.txt. The plugin's folder doesn't have any index.html file, hence on servers that have directory listing enabled, hackers can find and view the log:



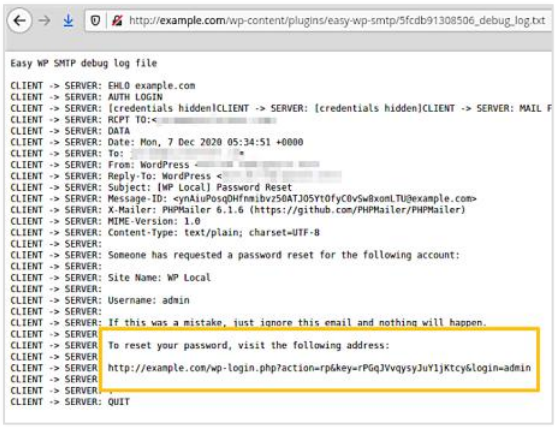
Then, they perform the usual username enumeration scans to find the admin login name, for instance via the REST API:



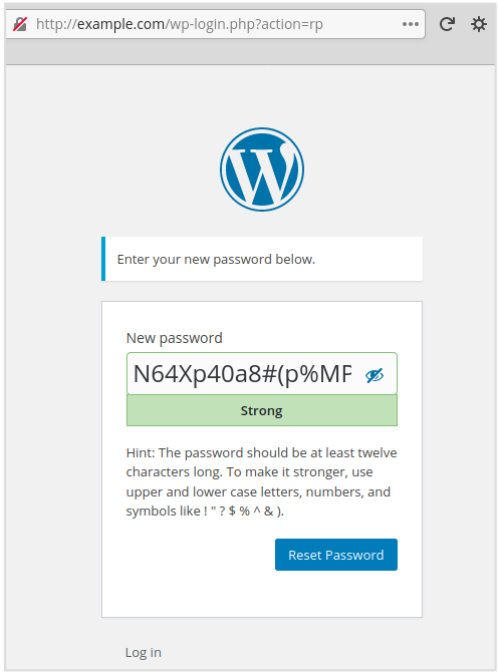
Hackers can also perform the same task using author achive scans (`/?author=1`).
They access the login page and ask for the reset of the admin password:



Then, they access the Easy WP SMTP debug log again in order to copy the reset link sent by WordPress:



With that link, they reset the admin password:



They log in to the admin dashboard and, on all WordPress hacked sites we saw, they immediately install rogue plugins on the blog.

Recommendations

Update immediately if you have version 1.4.2 or below installed.
Consider disabling the debug log, as it could leak sensitive information (messages, passwords etc).
If you are using our web application firewall for WordPress, NinjaFirewall WP Edition (free) and NinjaFirewall WP+ Edition (premium), you are protected against this vulnerability.

Stay informed about the latest vulnerabilities

- Running WordPress? You can get email notifications about vulnerabilities in the plugins or themes installed on your blog.
- On Twitter: @nintechnet

TAGGED: NINJAFIREWALL, SECURITY, VULNERABILITY, WORDPRESS

PREVIOUS

Authenticated RCE vulnerability in WordPress Secure File Manager plugin (unpatched).

NEXT

WordPress ListingPro theme fixed a critical vulnerability.

NinjaScanner

A lightweight, fast and powerful Antimalware scanner for WordPress which includes many features to help you scan your blog for malware and virus.

FREE DOWNLOAD

Code Profiler

Speed up your WordPress website by locating bottlenecks and performance issues in your plugins and themes.

FREE DOWNLOAD

CATEGORIES

Select Category

SEARCH

Search …

RECENT POSTS

1. WordPress FlyingPress plugin fixed broken access control vulnerability.
   November 28, 2022 - 12:13pm [+0700]
2. 8 WordPress plugins fixed high severity vulnerability.
   April 12, 2022 - 11:48am [+0700]
3. Unauthenticated function injection vulnerability in WordPress Sparkling theme.
   February 10, 2022 - 5:41pm [+0700]
4. Critical vulnerability in WordPress AdSanity plugin.
   January 25, 2022 - 12:17pm [+0700]
5. Code Profiler: WordPress Website Performance Profiling Made Easy.
   December 19, 2021 - 1:48am [+0700]