Chloe Chamberland

March 24, 2020

Vulnerabilities Patched in the Data Tables Generator by Supsystic Plugin

A few weeks ago, we disclosed several flaws that were patched in the Pricing Table by Supsystic plugin. On January 20th, our Threat Intelligence team discovered several similar vulnerabilities present in another product from Supsystic: Data Tables Generator by Supsystic, a WordPress plugin installed on over 30,000 sites. These flaws were very similar and allowed an attacker to execute several AJAX actions, inject malicious Javascript, and forge requests on behalf of an authenticated site user. However, in the Data Tables Generator plugin, these flaws required an attacker to be logged in as a user with subscriber or above permissions on a target site.

We privately disclosed these issues to the plugin's author at the same time we fully disclosed the flaws discovered in Pricing Table by Supsystic; again, they released patches a little over a month later. We recommend updating to the latest version, 1.9.92, immediately.

Wordfence Premium users received a new firewall rule on January 21, 2020 to protect against exploits targeting these vulnerabilities. Free Wordfence users received this rule on February 20, 2020.

Description: Insecure Permissions on AJAX Actions
Affected Plugin: Data Tables Generator by Supsystic
Plugin Slug: data-tables-generator-by-supsystic
Affected Versions: <= 1.9.91
CVE ID: CVE-2020-12075
CVSS Score: 6.3 (Medium)
CVSS Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L
Patched Version: 1.9.92

Data Tables Generator by Supsystic is an easy to use responsive table, chart, and data management plugin. It has several features such as custom css, the ability to add iframes, different fonts and label capabilities, and more. Unfortunately, we discovered that all of the AJAX actions to provide these features lacked capability checks and WordPress nonces for CSRF (Cross-Site Request Forgery) protection.

```
</pre>
<pre> /**
  * Validate and creates the new table.
  * @param Rsc_Http_Request $request
  * @return Rsc_Http_Response
  */
 public function createAction(Rsc_Http_Request $request)
 {
     $title = trim($request->post->get('title'));
     $rowsCount = (int) $request->post->get('rows');
     $colsCount = (int) $request->post->get('cols');

     try {
if (!$this->isValidTitle($title)) {
             return $this->ajaxError($this->translate('Title can\'t be empty or more than 255 characters'));
         }
$this->getEnvironment()->getModule('tables')->setIniLimits();
// Add base settings
         $tableId = $this->getModel('tables')->add(array('title' => $title, 'settings' => serialize(array())));

if($tableId) {
   $rows = array();

   for($i = 0; $i < $rowsCount; $i++) {
      array_push($rows, array('cells' => array()));
      for($j = 0; $j < $colsCount; $j++) {
         array_push($rows[$i]['cells'], array(
            'data' => '',
            'calculatedValue' => '',
                         'hidden' => '',
                      'type' => 'text',
                      'formatType' => '',
            'meta' => array()
         ));
      }
   }
   // Save an empty table's rows to prevent error when the Data Tables script will be executed
   $this->getModel('tables')->setRows($tableId, $rows);
}
     } catch (Exception $e) {
         return $this->ajaxError($e->getMessage());
     }

     return $this->ajaxSuccess(array('url' => $this->generateUrl('tables', 'view', array('id' => $tableId))));
 }</pre>
<pre>
```

**One example of a function triggered by the AJAX action `create`. No nonce or permission checks present.

WordPress AJAX actions can be processed by any authenticated user. As such, AJAX actions should always require an additional capability check in order to verify that the user sending the request is an authenticated administrative user when the action is meant for only administrative users. Without the required permission check, any user logged in as subscriber or above could execute the actions and make malicious changes to any given data table, or create a new data table. With many sites allowing open subscriber registrations, protecting site functionality with capability checks is critical when utilizing AJAX actions.

The vulnerable endpoints we discovered were: `getListForTbl`, `updateRows`, `updateMeta`, `saveSettings`, `remove`, `create`, `render`, `getSettings`, `getMeta`, `getCountRows`, `getRows`, `clone`, and `rename`. The most impactful endpoints were `rename`, where an attacker could rename any given data table name, `getListForTbl`, where an attacker could discover all of the existing tables and use that information to craft a request, `saveSettings`, where an attacker could modify any data table settings maliciously, and `create`, where an attacker could create a new data table with any options set.

Description: Authenticated Stored XSS
Affected Plugin: Data Tables Generator by Supsystic
Affected Versions: <= 1.9.91
CVE ID: CVE-2020-12075
CVSS Score: 5.4 (Medium)

CVSS Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N
Patched Version: 1.9.92

table fields, including the title, the data table cells, the description and caption, and more, by using the `saveSettings` endpoint to update an existing data table.

The malicious Javascript would then execute in a site visitor's browser whenever they accessed a page containing the data table. This could ultimately lead to malicious site redirection, new administrative user account creation, and other malicious actions.

As previously mentioned with the Pricing Table by Supsystic plugin, WordPress allows default administrators the capability to use `unfiltered_html`. Alone, these settings would not be considered a security risk if only administrative users had access to modify these settings. However, providing the `unfiltered_html` capability with these AJAX actions that allowed even subscriber-level users to modify these settings introduced a cross site scripting (XSS) vulnerability.

Description: CSRF to Stored XSS, Data Table Creations, Settings Modification
Affected Plugin: Data Tables Generator by Supsystic
Plugin Slug: data-tables-generator-by-supsystic
Affected Versions: <= 1.9.91
CVE ID: CVE-CVE-2020-12076
CVSS Score: 8.8 (High)
CVSS Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H
Patched Version: 1.9.92

The lack of WordPress nonces for CSRF protection on all actions registered in this plugin also resulted in several Cross-Site Request Forgery (CSRF) vulnerabilities. Given that the registered actions could be executed by any logged-in user regardless of privilege level, CSRF exploit attempts could be targeted towards any user, even those with just a subscriber role.

If an attacker was able to trick any authenticated user into clicking on a link or opening a malicious attachment, a forged request could be sent on behalf of that user to modify any given data table and inject malicious Javascript. Again, the malicious Javascript could inject a new administrative user, redirect site visitors to a malicious site, and more.

It is important to remember not to click on links in comments or emails unless you can verify the authenticity of the source and the destination to protect against a CSRF exploit attempt. It is difficult for firewalls to protect against CSRF attacks because the malicious request appears to come from a valid, authenticated user.

Disclosure Timeline

January 20, 2020 – Vulnerability initially discovered and analyzed. We begin working on firewall rules.
January 21, 2020 – Firewall rule released for Wordfence premium users. Awaiting response from the Supsystic's plugin team in regards to vulnerabilities in Pricing Table by Supsystic.
January 21, 2020 – Plugin team confirms appropriate inbox for handling discussion. Full disclosure of vulnerabilities is sent.
January 30, 2020 – Follow-up with plugin team as no response from disclosure.
February 11, 2020 – Plugin developer acknowledges report.
February 20, 2020 – Wordfence free users receive firewall rule.
February 21, 2020 – Additional and final follow-up. Insufficient patch released.
February 21 to March 23, 2020 – Back and forth with the plugin team to ensure an optimal solution released.
March 23, 2020 – Final patch released.

Conclusion

In today's post, we detailed several vulnerabilities including stored XSS, CSRF, and insecure permissions found in the Data Tables by Supsystic plugin. These flaws have been fully patched in version, 1.9.92, and we recommend that users update to the latest version available immediately. Sites running Wordfence Premium have been protected from attacks against this vulnerability since January 21, 2020. Sites running the free version of Wordfence received the firewall rule update on February 20, 2020.
Did you enjoy this post? Share it!

Comments

No Comments