JASK

THREAT ADVISORY

Drupalgeddon2 CVE-2018-7600

AUTHOR
ROD SOTO

JASKLABS
TA-00011

TLP
WHITE

RISK FACTOR
HIGH

THREAT ADVISORY

Drupalgeddon2
CVE-2018-7600

AUTHOR
ROD SOTO

JASKLABS
TA-00011

TLP
WHITE

RISK FACTOR

HIGH

Overview

A new Drupal critical vulnerability has been published CVE-2018-7600. This vulnerability allows unauthenticated attacker to execute code remotely, this can lead to a complete take over of targeted website. Drupal is a very popular content management system framework (CMS), just like wordpress or joomla. It is said that this vulnerability impacts over 1 Million sites.

Indicators

Drupal versions 8, 7, and 6 sites are affected according to Drupal security team. (See more on Mitigation section).

According to Drupal security team this is a Highly Critical vulnerability with a CMSS score of 21/25
AC:None/A:None/CI:All/II:All/E:Theoretical/TD:Default.

The scoring above highlights the following items that make this vulnerability highly critical:

- Anonymous access (No need for authentication).
- Can be triggered remotely (No need of local access).
- Makes all data accessible (Public AND non public).
- Data can not only be accessed but modified or even deleted.
- Targeted site can be taken over.

Lab Study

This vulnerability was discovered by Japer Mattsson, and as of the writing of this advisory, there are no public exploits or known exploitation in the wild. However, it is known that malicious actors and professional criminals can and will reverse engineer published patches in order to replicate vulnerabilities and create exploit code.

According to Wordfence by looking for the differences in the code in between patches there is an observable new class "DrupalRequestSanitizer" which is related to sanitizing or controlling input in the following code parameters.

AUTHOR
ROD SOTO

JASKLABS
TA-00011

TLP
WHITE

RISK FACTOR
HIGH

Fig Shows Drupal patch for CVE-2018-7600

```
+  protected static function stripDangerousValues($input, array $whitelist, array &$sanitized_keys) {
+    if (is_array($input)) {
+      foreach ($input as $key => $value) {
+        if ($key !== '' && $key[0] === '#' && !in_array($key, $whitelist, TRUE)) {
+          unset($input[$key]);
+          $sanitized_keys[] = $key;
+        }
+        else {
+          $input[$key] = static::stripDangerousValues($input[$key], $whitelist, $sanitized_keys);
+        }
+      }
+    }
+    return $input;
+  }
+
+}
```

It is a matter of time until proof of concept exploit code is published and eventually used for mass exploitation.

JASK Detection

As of the writing of this advisory there are no public proof of concepts of this exploit available. However we can speculate based on the difference in code shown above, that exploit could be in the form of $GET or $POST request, which according to code can be translated into $input array/key that previous code did not sanitize.

If exploit contains key or values being passed via $input then we can use ASOC to capture exploit attempts via a number of requests or specific values in those requests ($REQUEST). The following figure shows JASK ASOC patterns targeting specific requests for detection.

Figure Shows First Seen Access signal

2018-04-03 04:32:00 EDT	104.236.55.48	104.236.47.73	45688	8080	GET http://akdkidsbeylikduzu.com/modules/pk_vertflexmenu/config.xml	302 Found

HTTP REQUEST

```
GET /modules/pk_vertflexmenu/config.xml HTTP/1.1
Cache-Control: max-age=259200
Connection: keep-alive
Host: akdkidsbeylikduzu.com
User-Agent: Mozilla/5.0 (compatible; MSIE 6.0; Windows NT 5.1; Trident/4.0)
X-Forwarded-For: unknown
```

HTTP RESPONSE

```
HTTP/1.1 302 Found
Cache-Control: no-cache
Connection: keep-alive
Content-Length: 230
Content-Type: text/html; charset=iso-8859-1
Date: Tue, 03 Apr 2018 08:32:32 GMT
Expires: Tue, 03 Apr 2018 08:32:32 GMT
Location: http://www.akdkidsbeylikduzu.com/error404.html
Pragma: no-cache
Server: nginx
X-Cache: MISS from labl-sensor01-nyc3
X-Cache-Lookup: MISS from labl-sensor01-nyc3:8080
```

2018-04-03 04:32:00 EDT	104.236.55.48	104.236.47.73	45634	8080	GET http://www.jzgcjsys.com/	503 Service Unavailable
2018-04-03 04:32:00 EDT	104.236.55.48	104.236.47.73	45546	8080	GET http://www.jzgcjsys.com/	503 Service Unavailable
2018-04-03 04:32:00 EDT	104.236.55.48	104.236.47.73	45570	8080	GET http://www.jzgcjsys.com/	503 Service Unavailable

Rows per page: 10 1-10 of 68

AUTHOR
ROD SOTO

JASKLABS
TA-00011

TLP
WHITE

RISK FACTOR

HIGH

Once we identify specific values we can refine detection pattern via JASK ASOC investigation tools, and use other contextual elements such as unusual connections, frequency of connections, URI entropy, webshell/C2 type of traffic, IP reputation, Threat Intelligence, and many other sources of data that can be used to provide a complete picture of detection and management of this vulnerability.

Mitigation

Fig Shows Drupal Security team mitigation route.

Upgrade to the most recent version of Drupal 7 or 8 core.

- **If you are running 7.x, upgrade to Drupal 7.58.** (If you are unable to update immediately, you can attempt to apply this patch to fix the vulnerability until such time as you are able to completely update.)
- **If you are running 8.5.x, upgrade to Drupal 8.5.1.** (If you are unable to update immediately, you can attempt to apply this patch to fix the vulnerability until such time as you are able to completely update.)

Drupal 8.3.x and 8.4.x are no longer supported and we don't normally provide security releases for unsupported minor releases. However, given the potential severity of this issue, we *are* providing 8.3.x and 8.4.x releases that includes the fix for sites which have not yet had a chance to update to 8.5.0.

Your site's update report page will recommend the 8.5.x release even if you are on 8.3.x or 8.4.x. Please take the time to update to a supported version after installing this security update.

- If you are running 8.3.x, upgrade to Drupal 8.3.9 or apply this patch.
- If you are running 8.4.x, upgrade to Drupal 8.4.6 or apply this patch.

This issue also affects Drupal 8.2.x and earlier, which are no longer supported. If you are running any of these versions of Drupal 8, update to a more recent release and then follow the instructions above.

This issue also affects Drupal 6. Drupal 6 is End of Life. For more information on Drupal 6 support please contact a D6LTS vendor.

The above mitigation route should help mitigate this specific vulnerability and must be applied ASAP in anticipation of exploit code made available.

The are also a number of other mitigation features that have been announced by the security community that might be specific to the use of certain web application firewall technology and security vendors are applying signatures of this attack based on review of the code shown in the Lab study.