
DrupalEurope
Darmstadt, Germany
Sep 10 - 14, 2018
www.drupaleurope.org

Drupal Europe
Darmstadt, Germany
10 - 14 September 2018

No photos please

Responsible disclosure, cross-project collaboration, and Drupal 8 security

xjm

Drupal & Technology | http://bit.ly/drupal-europe-d8-security

Drupal Europe
Darmstadt, Germany
10 - 14 September 2018

Drupal + Technology

TRACK SUPPORTED BY

platform.sh

"Statue" of me, from yched

I'm xjm

Drupal 8 release manager

Drupal Security Team member

Code & Community Strategist, Acquia

drupal.org/u/xjm

@xjmdrupal

Drupal Europe
Darmstadt, Germany
10 - 14 September 2018

Drupal Europe
Darmstadt, Germany
Sep 10 - 14, 2018

What is responsible disclosure?

"...A vulnerability is disclosed only after a period of time that allows for the vulnerability to be patched."

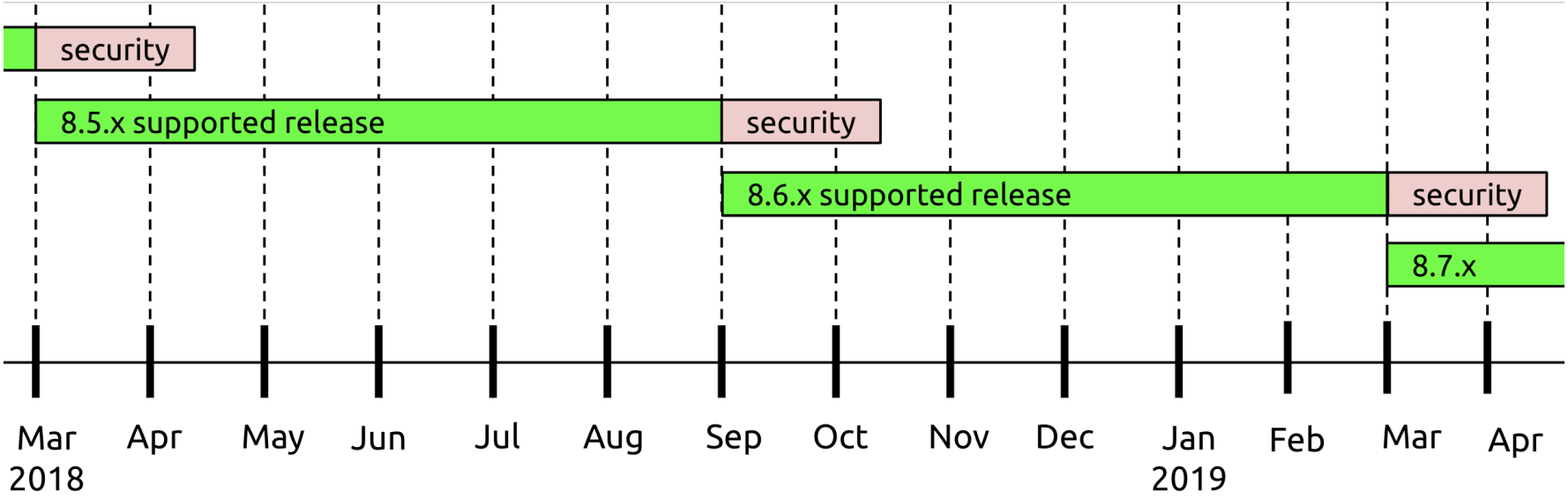
Wikipedia

Drupal security release windows

Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	1	2	3	4	5

Modern tooling

Semantic versioning, 6-month release cycle



Drupal 8 coordinates releases with:

- Drupal 7
- Contributed projects
- Upstream dependencies
- Other OS projects (Backdrop, WordPress...)

Drupal Europe
Darmstadt, Germany
Sep 10 - 14, 2018

Security release challenges and successes

(As illustrated by past Drupal 8 security advisories)

httpoxy & Guzzle

SA-CORE-2016-003

Drupal 8.1.7, July 2016

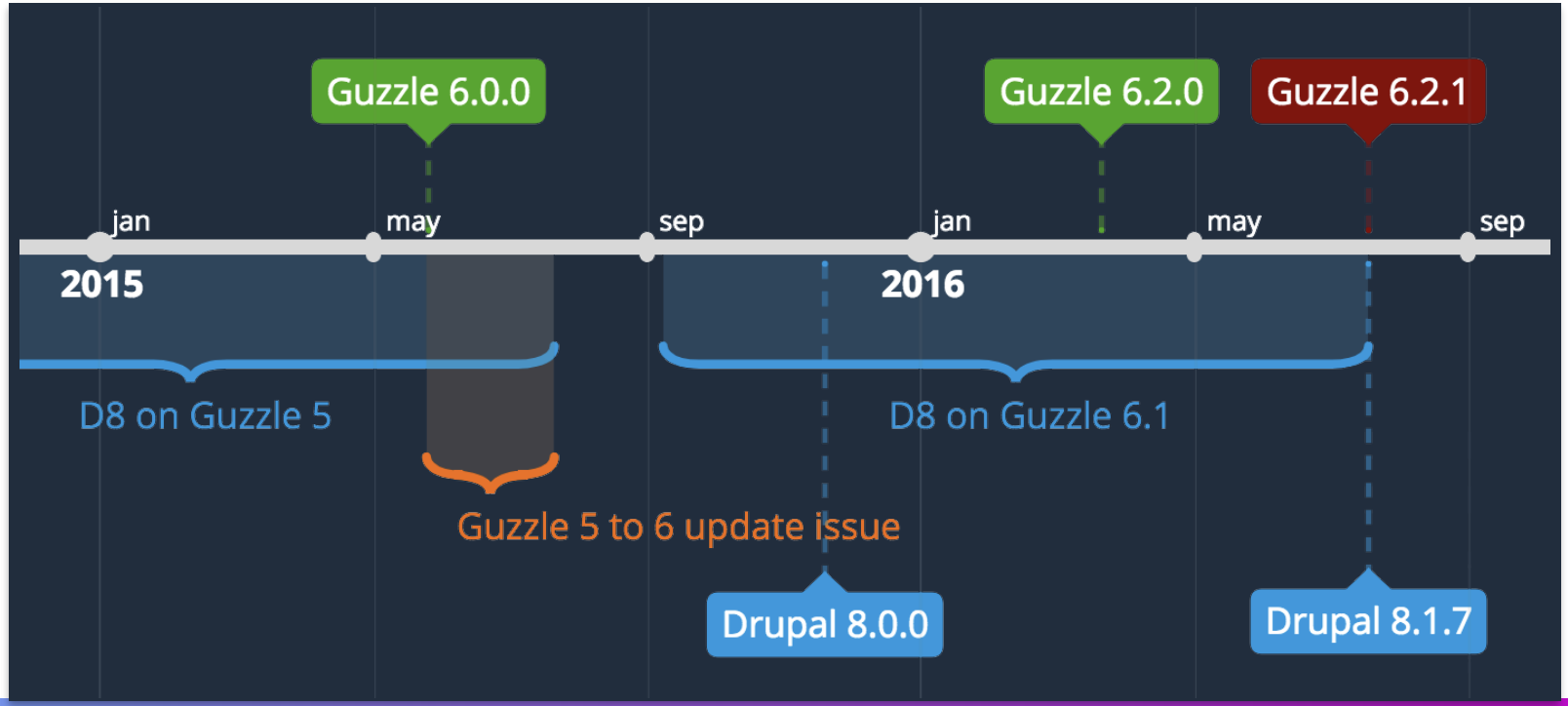
httpoxy & Guzzle

Fixed in Guzzle 6.2.1


```
- if ($proxy = getenv('HTTP_PROXY')) {
-   $defaults['proxy']['http'] = $proxy;
+ if (php_sapi_name() == 'cli' && getenv('HTTP_PROXY')) {
+   $defaults['proxy']['http'] = getenv('HTTP_PROXY');
```

httpoxy & Guzzle

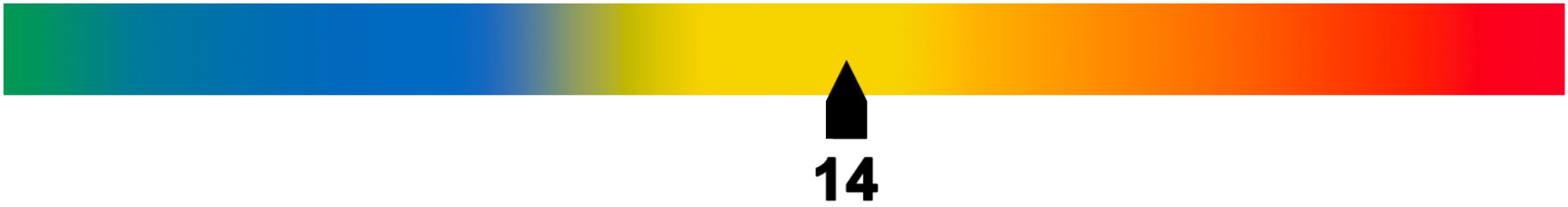
Fixed in Guzzle 6.2.1



httpoxy & Guzzle

Fixed in Guzzle 6.2.1

PHPUnit RCE



SA-CORE-2017-001

Drupal 8.2.7, March 2017

(packaging change December 2016)

PHPUnit RCE

Drupal.org packaging change

Drupal 8 will no longer include dev dependencies in release packages

Posted by xjm on *12 November 2016*

As a best practice, development tools should not be deployed on production sites. Accordingly, packaged Drupal 8 stable releases will no longer contain development PHP libraries, because

PHPUnit RCE

Fixed in PHPUnit 4.8.28

```
<?php

- eval('?>' . file_get_contents('php://input'));
+ eval('?>' . file_get_contents('php://stdin'));
```

PHPUnit RCE

CLI functionality

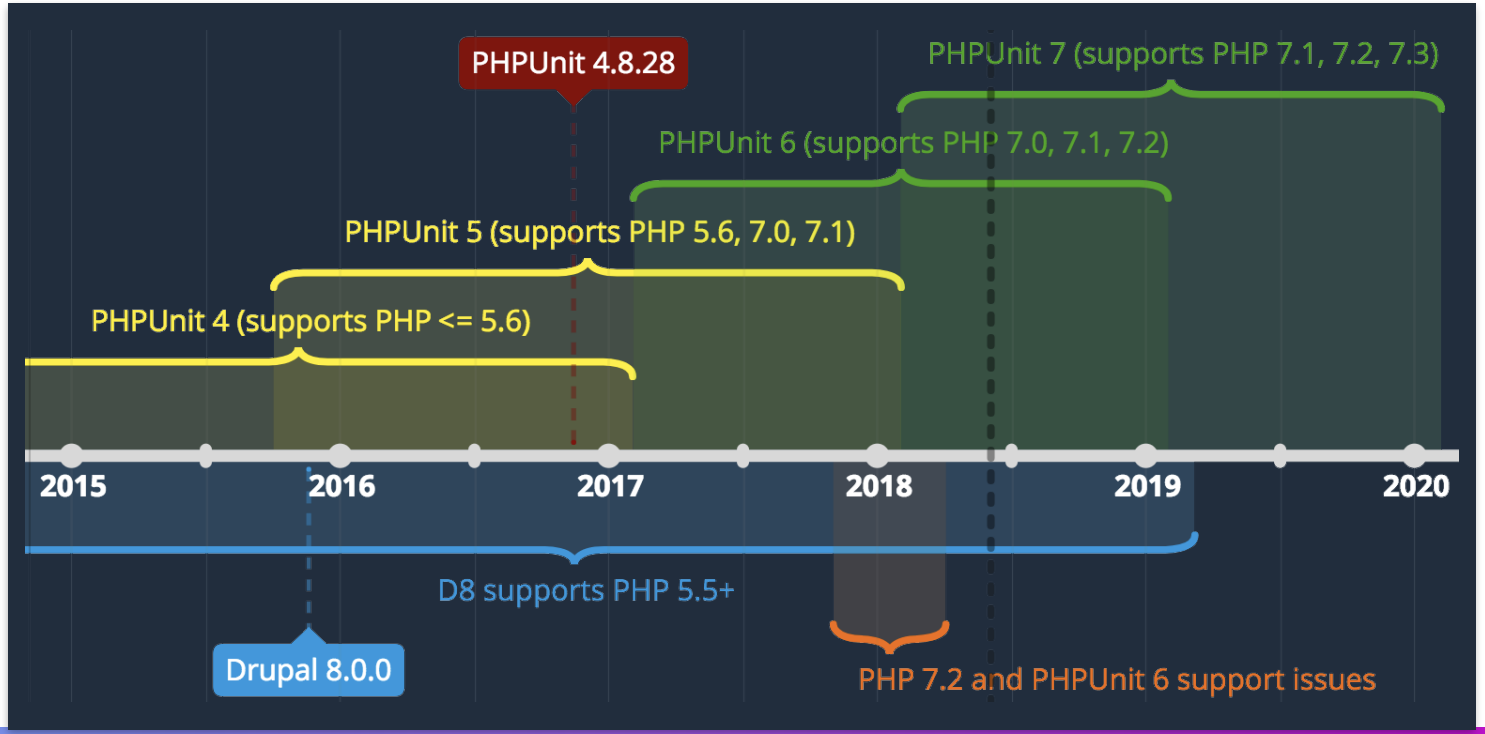

```
<?php

- eval('?>' . file_get_contents('php://input'));
+ eval('?>' . file_get_contents('php://stdin'));
```

Compare:

```
- if ($proxy = getenv('HTTP_PROXY')) {
-   $defaults['proxy']['http'] = $proxy;
+ if (php_sapi_name() == 'cli' && getenv('HTTP_PROXY')) {
+   $defaults['proxy']['http'] = getenv('HTTP_PROXY');
```

PHPUnit RCE

Fixed in PHPUnit 4.8.28



jQuery 2 Ajax XSS

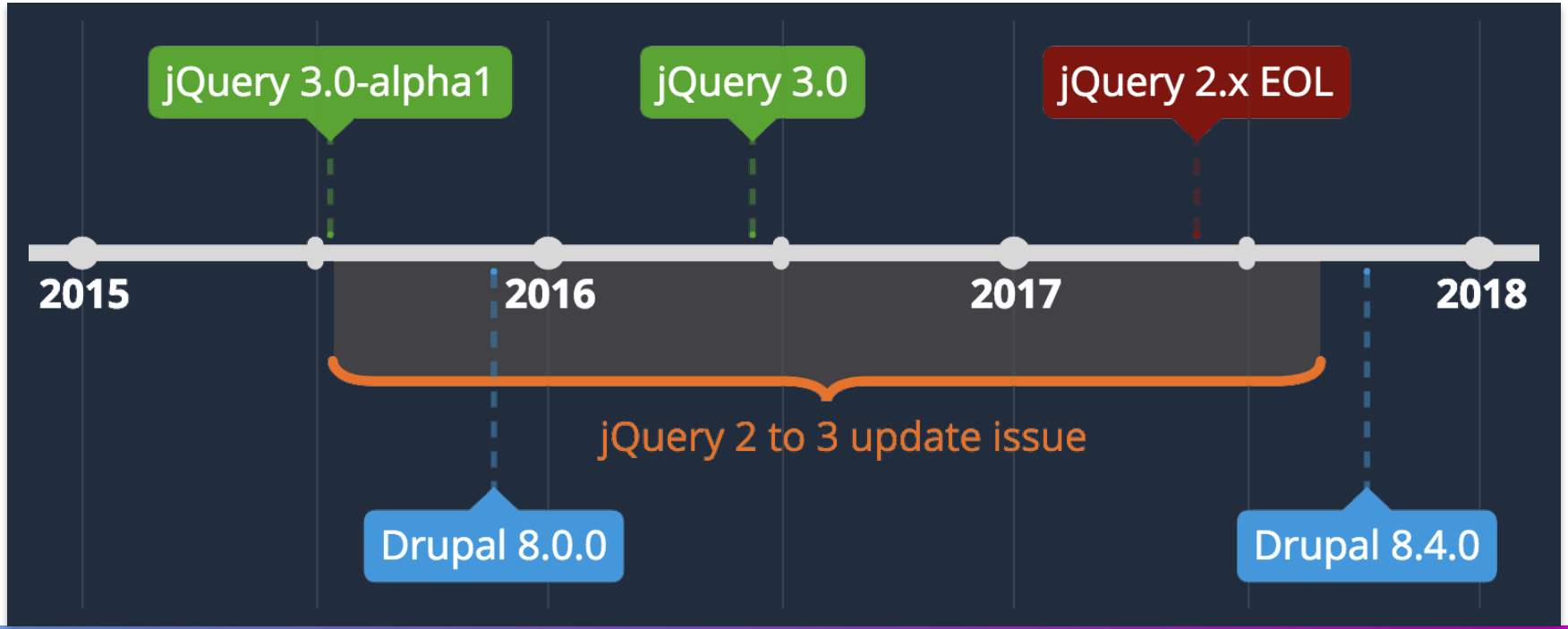
No Drupal 8 SA

Drupal 8.4.0, October 2017

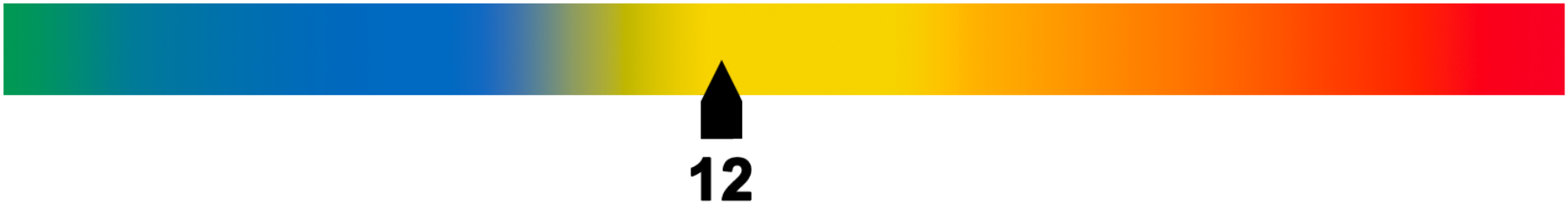
(D7 mitigation in SA-CORE-2018-001)

jQuery 2 Ajax XSS

Drupal Europe
Darmstadt, Germany
10 - 14 September 2018



CKEditor stored XSS (img alt attribute)



SA-CORE-2018-003

Drupal 8.5.2, April 2018

(Thank you mlewand and wwalc!)

REST entity vulnerability #1: Entity access bypass

SA-CORE-2017-002

Drupal 8.3.1 and 8.2.8, April 2017

REST entity vulnerability #1: Entity access bypass


```
+ if ($operation === 'edit') {
+   if ($field_definition->getName() === $this->entityType->getKey('id')) {
+     return $return_as_object
+       ? AccessResult::forbidden('The entity ID cannot be changed')
+       : FALSE;
+   }
+   elseif ($field_definition->getName() ===
+     $this->entityType->getKey('uuid')) {
+     if ($items && ($entity = $items->getEntity()) && !$entity->isNew()) {
+       return $return_as_object
+         ? AccessResult::forbidden('The entity UUID cannot be changed')
+           ->addCacheableDependency($entity)
+         : FALSE;
+     }
+   }
+ }
```

REST entity vulnerability #1: Entity access bypass

Drupal 8.2

Nodes vulnerable

http://bit.ly/sam-rest-security

REST entity vulnerability #1: Entity access bypass

Drupal 8.2

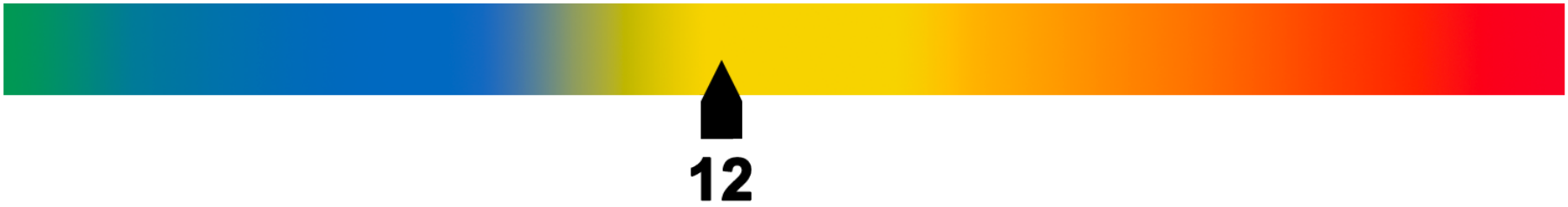
Nodes vulnerable

Drupal 8.3

Users vulnerable

http://bit.ly/sam-rest-security

REST entity vulnerability #2: Missing file validation

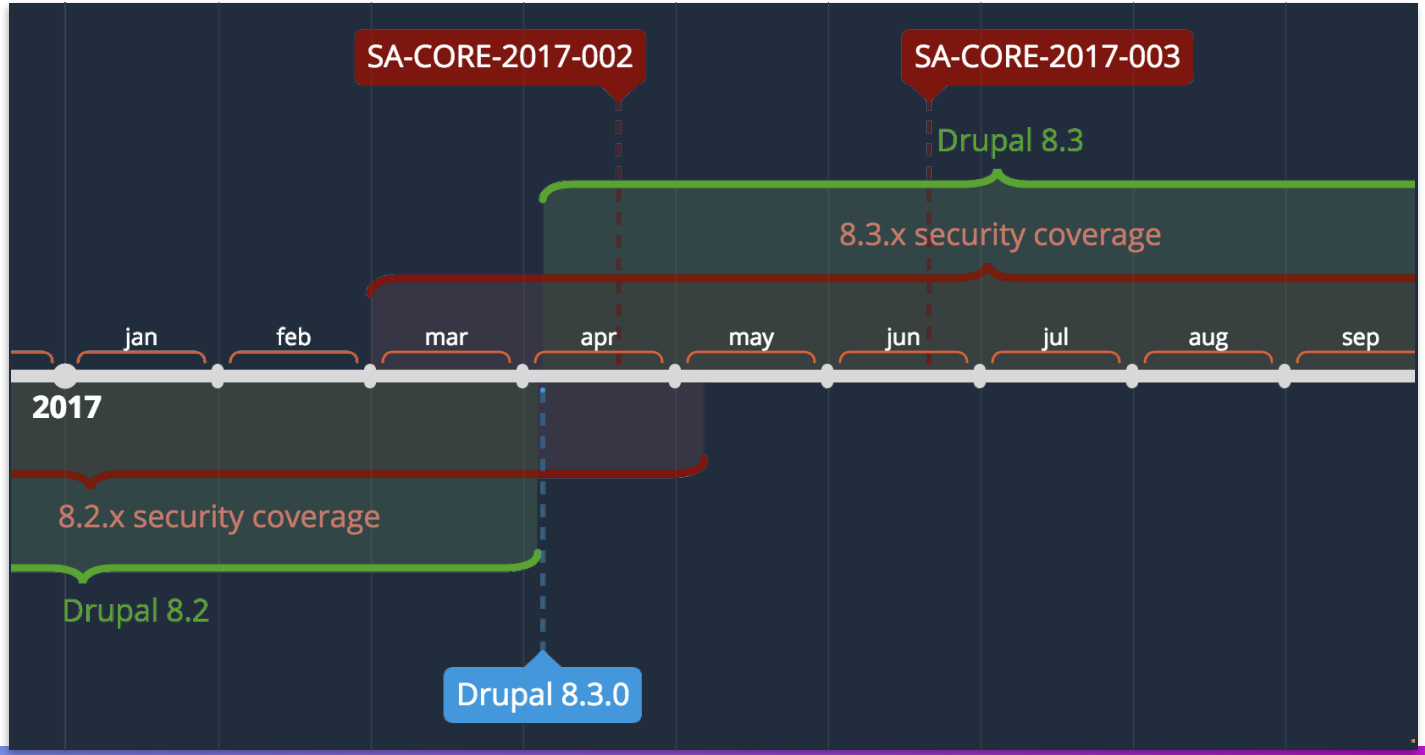


SA-CORE-2017-003

Drupal 8.3.4, June 2017

**Note: Score shown here differs from the published SA*

REST entity vulnerability #2: Missing file validation



REST entity vulnerability #2: Missing file validation


```
+ $create_only_fields = [
+   'uri',
+   'filemime',
+   'filesize',
+ ];
+ $field_name = $field_definition->getName();
+ if ($operation === 'edit' && $items && ($entity = $items->getEntity())
+   && !$entity->isNew()
+   && in_array($field_name, $create_only_fields, TRUE)) {
+   return AccessResult::forbidden();
+ }
```

REST entity vulnerability #3: Comment approval bypass

SA-CORE-2017-004

Drupal 8.3.7, August 2017

REST entity vulnerability #3: Comment approval bypass

Drupal Europe
Darmstadt, Germany
10 - 14 September 2018

```
if (is_null($this->get('status')->value)) {
  if (\Drupal::currentUser()->hasPermission('skip comment approval')) {
    $this->setPublished();
  }
```

(image credit: arshadcn)

REST entity vulnerability #3: Comment approval bypass


```
   parent::preSave($storage);
- if (is_null($this->get('status')->value)) {
-   if (\Drupal::currentUser()->hasPermission('skip comment approval')) {
-     $this->setPublished();
-   }
-   else {
-     $this->setUnpublished();
-   }
- }
+ $fields['status']->setDefaultValueCallback(
+   'Drupal\comment\Entity\Comment::getDefaultStatus'
+ );

+ public static function getDefaultStatus() {
+   return \Drupal::currentUser()->hasPermission('skip comment approval')
+     ? CommentInterface::PUBLISHED
+     : CommentInterface::NOT_PUBLISHED;
+  }
```

Highly critical remote code execution in Drupal 7 and Drupal 8

Drupal Europe
Darmstadt, Germany
10 - 14 September 2018

SA-CORE-2018-002

Drupal 8.5.1, 8.4.6, 8.3.9, & 7.58

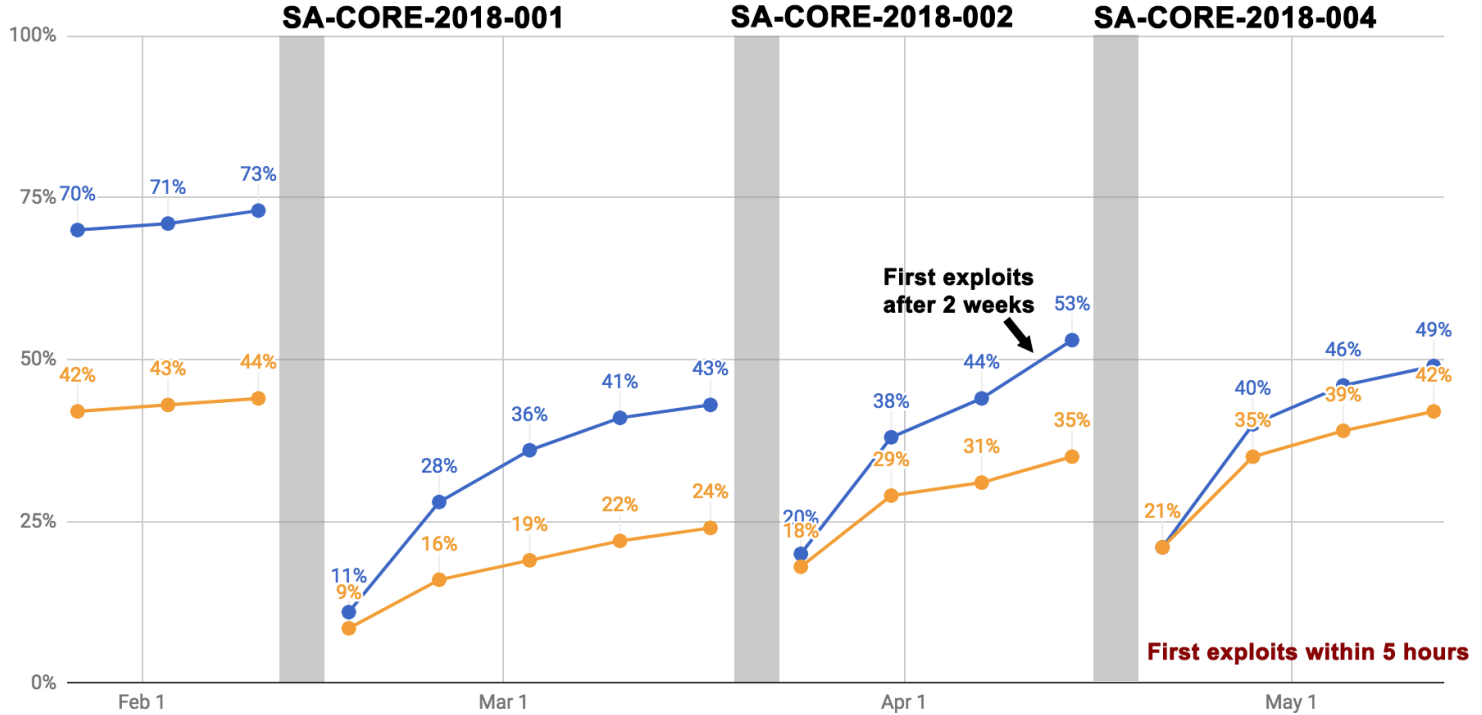
March 2018 (followup April 2018)

https://www.drupaleurope.org/session/autopsy-vulnerabilities

Highly critical remote code execution in Drupal 7 and Drupal 8

Drupal Europe
Darmstadt, Germany
10 - 14 September 2018

Sites on secure, tagged releases after each SA



Drupal Europe
Darmstadt, Germany
Sep 10 - 14, 2018

Lessons

What have we learned?
How can we improve?

Effective coordinated disclosure is *hard*

Wendy Nather
@wendynather

Follow

OH: Coordinated disclosure is like conducting an orchestra where half the musicians don't show up and the other half are playing a song they never heard before

Also, some musicians deny they're playing instruments. And the woodwinds section is on fire

9:03 AM - 28 Feb 2018

70 Retweets **225** Likes

We can't always set the schedule

We must avoid single points of failure.
Cross-project relationships are essential.

We have to deal with BC breaks in dependency updates

jQuery3 broke stuff.
Symfony broke more.
We needed both.

https://www.thirdandgrove.com/long-road-drupal-9

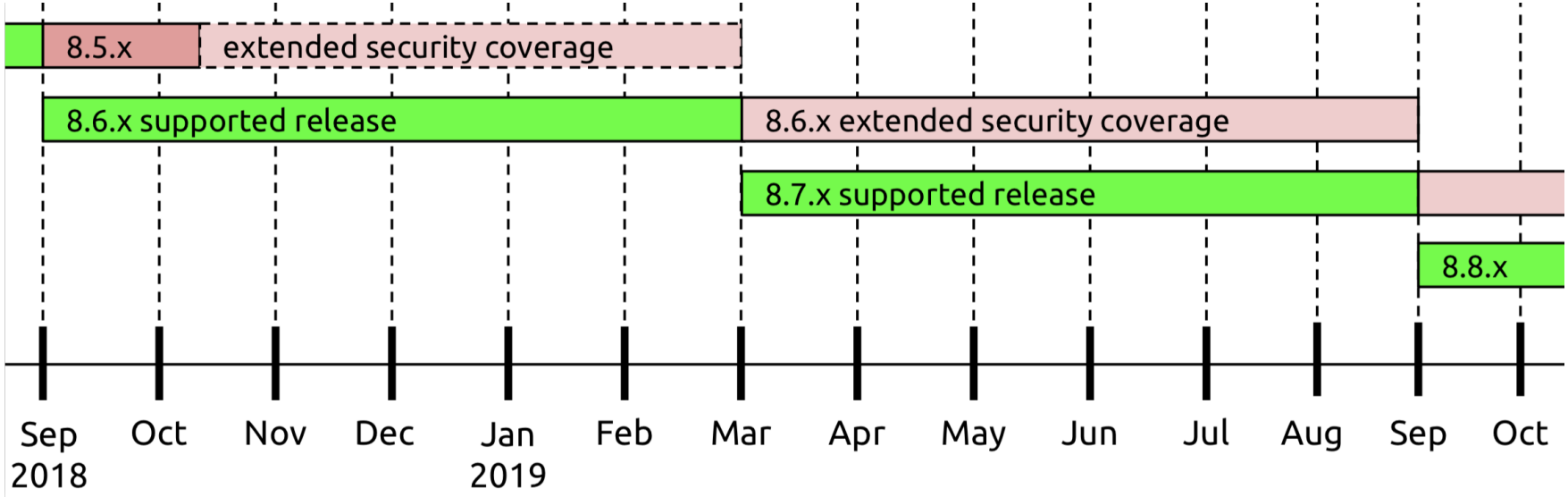
We need (secure) automatic updates for security issues

This is not simple to solve.

https://www.drupal.org/initiatives/automatic-updates

http://bit.ly/hacking-wordpress-autoupdate

New policy: Overlapping security coverage for minor versions



https://www.drupal.org/node/2909665

New vulnerabilities and attack vectors

Drupal 8 APIs are new and evolving.
Vulnerabilities evolve along with them.

Drupal Europe
Darmstadt, Germany
Sep 10 - 14, 2018

Become a Drupal contributor Friday from 9am

- First-time contributor workshop
- Mentored contributions
- General contributions

Thanks to...

- mlhess
- greggles
- samuel.mortenson
- pwolanin
- David_Rothstein
- David Strauss
- dsnopek
- Wim Leers
- Josh Koenig
- Jasu_M
- mlewand and wwalc
- The Boston Drupal Group
- Drupal HackCamp
- Issue reporters
- The Drupal Security Team