Drupal Site Maintenance & Security

Ryann Levo & Stacy Pendell
Custom Development
Cornell Information Technologies

Keeping Drupal up to date

- Drupal core and modules have regular updates
  - Announced by their developers
- Security updates may need quick action to keep site safe
  - Easier to do if site is up to date overall

Why security is important

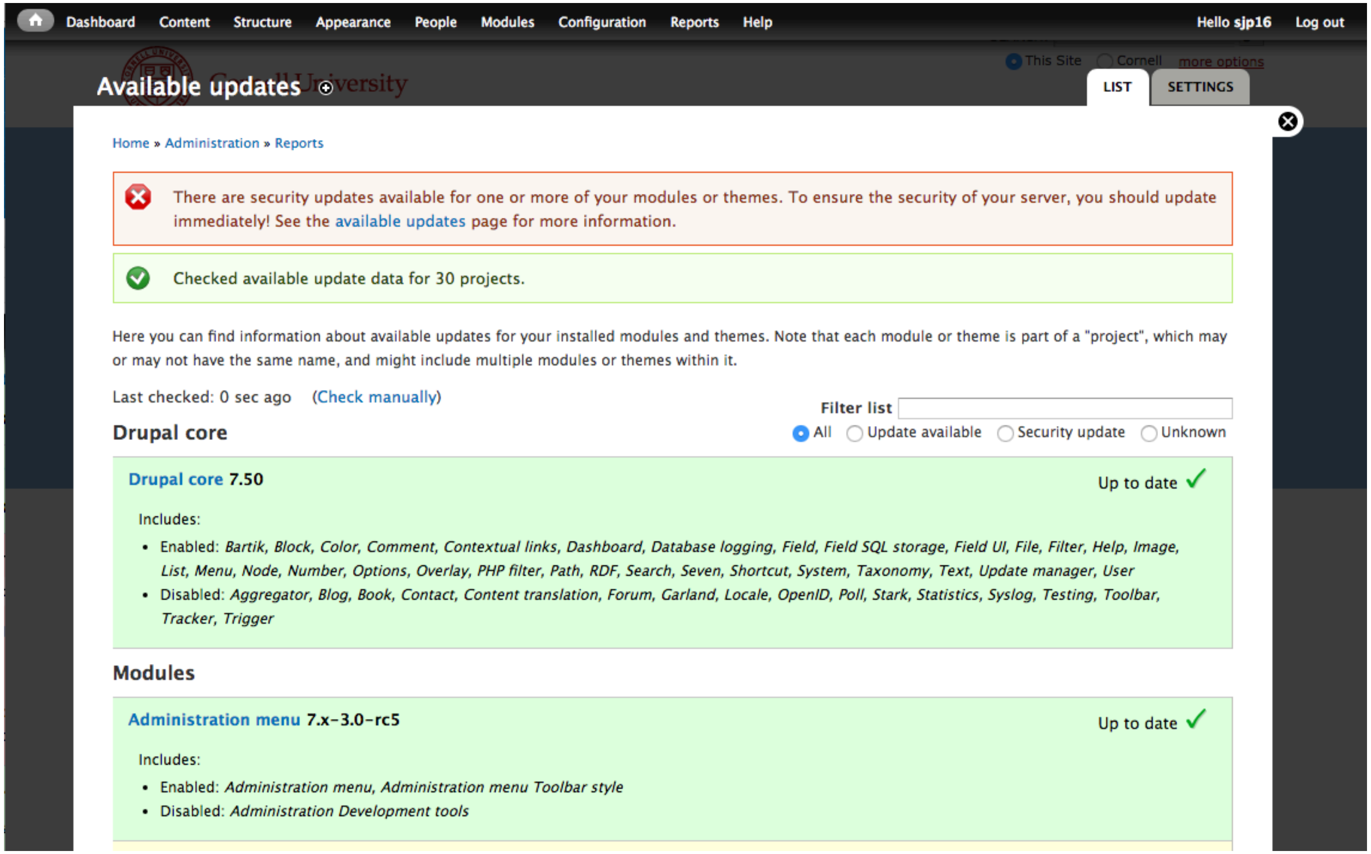
- Attackers scan and probe sites constantly
  - Looking for ways to steal credentials or insert links
  - Spammers scanning for email addresses can overload a site, causing it to slow down or crash
- Security experts provide a fix or patch when they announce a newly discovered vulnerability, but attackers move quickly

Where to get help

- For Cornell sites, the IT Security Office can help
- Scan sites regularly for vulnerabilities
- Amount of work to prevent an attack is way less than work to recover a compromised site

Check site for core and module updates

- Admin menu / Reports / Available updates



Available updates

Home » Administration » Reports

There are security updates available for one or more of your modules or themes. To ensure the security of your server, you should update immediately! See the available updates page for more information.

Checked available update data for 30 projects.

Here you can find information about available updates for your installed modules and themes. Note that each module or theme is part of a "project", which may or may not have the same name, and might include multiple modules or themes within it.

Last checked: 0 sec ago (Check manually)

Filter list

● All ○ Update available ○ Security update ○ Unknown

Drupal core

Drupal core 7.50 — Up to date ✓

Includes:

- Enabled: *Bartik, Block, Color, Comment, Contextual links, Dashboard, Database logging, Field, Field SQL storage, Field UI, File, Filter, Help, Image, List, Menu, Node, Number, Options, Overlay, PHP filter, Path, RDF, Search, Seven, Shortcut, System, Taxonomy, Text, Update manager, User*
- Disabled: *Aggregator, Blog, Book, Contact, Content translation, Forum, Garland, Locale, OpenID, Poll, Stark, Statistics, Syslog, Testing, Toolbar, Tracker, Trigger*

Modules

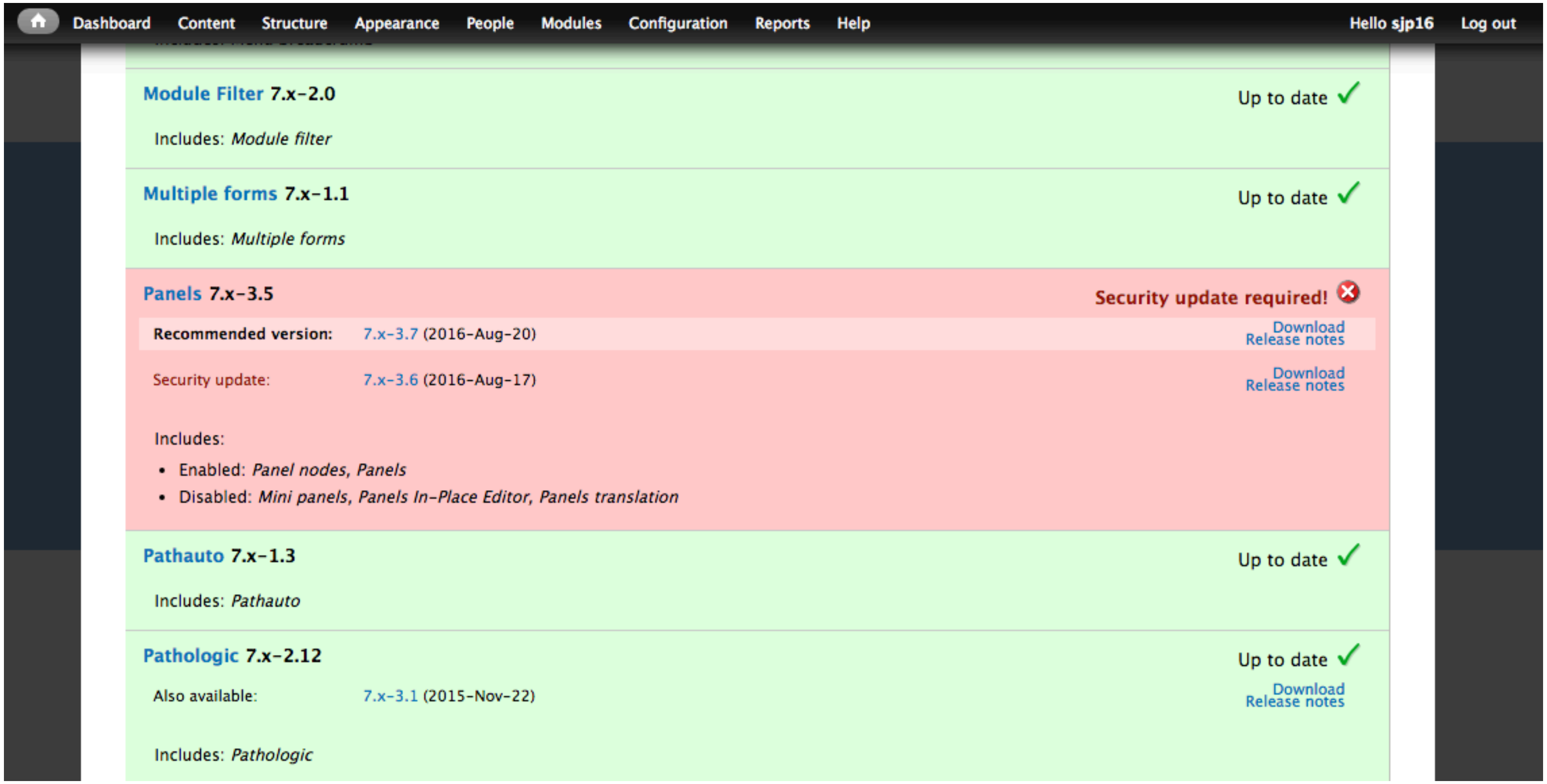
Administration menu 7.x-3.0-rc5 — Up to date ✓

Includes:

- Enabled: *Administration menu, Administration menu Toolbar style*
- Disabled: *Administration Development tools*

Scroll down to check all updates

- Security updates have red background
- Red could also mean a module is no longer supported by its developers



Module Filter 7.x-2.0 — Up to date ✓

Includes: *Module filter*

Multiple forms 7.x-1.1 — Up to date ✓

Includes: *Multiple forms*

Panels 7.x-3.5 — Security update required! ☒

Recommended version:	7.x-3.7 (2016-Aug-20)	Download Release notes
Security update:	7.x-3.6 (2016-Aug-17)	Download Release notes

Includes:
- Enabled: *Panel nodes, Panels*
- Disabled: *Mini panels, Panels In-Place Editor, Panels translation*

Pathauto 7.x-1.3 — Up to date ✓

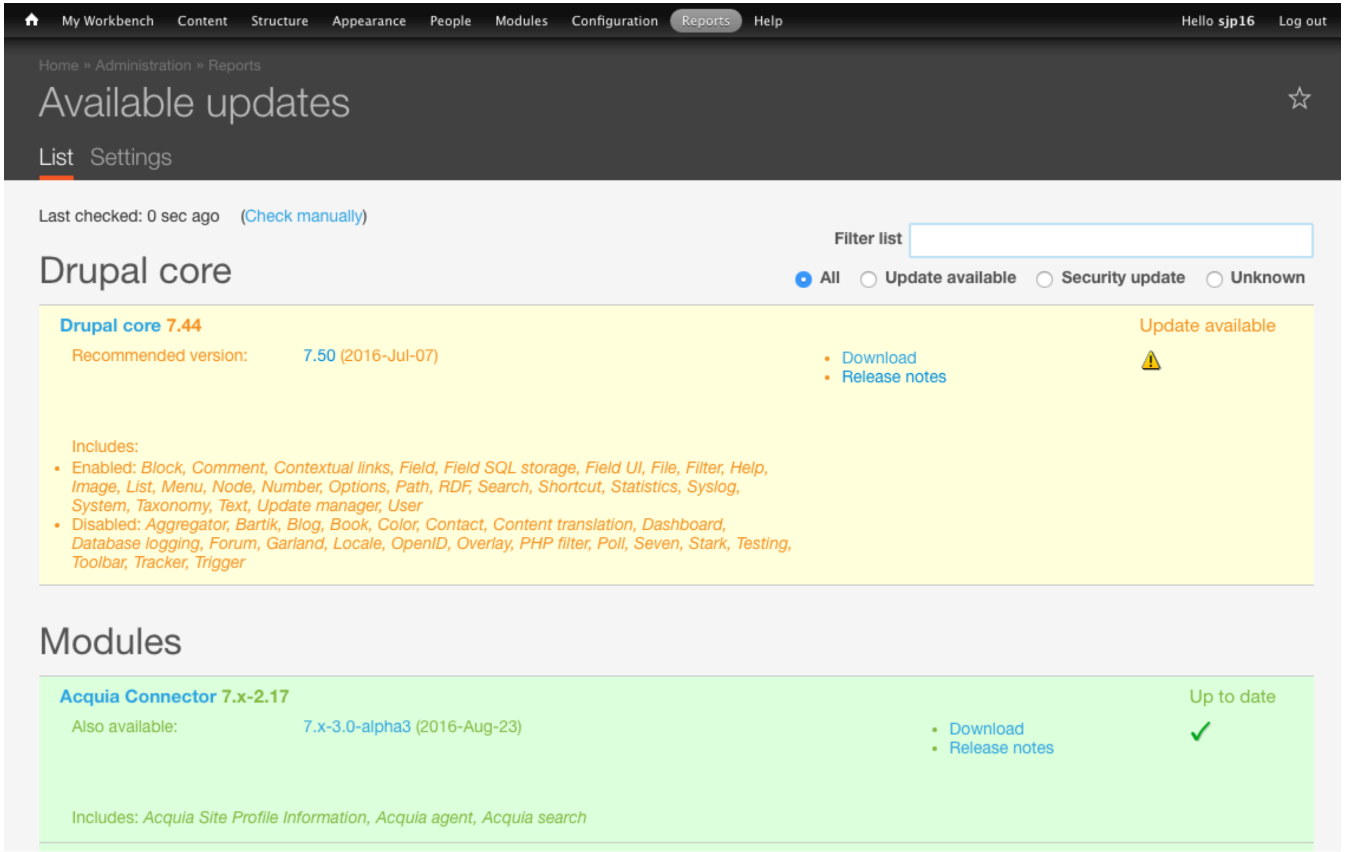
Includes: *Pathauto*

Pathologic 7.x-2.12 — Up to date ✓

Also available:	7.x-3.1 (2015-Nov-22)	Download Release notes

Includes: *Pathologic*

- Non-security updates are tan or yellow



Available updates

Last checked: 0 sec ago (Check manually)

Filter list

● All ○ Update available ○ Security update ○ Unknown

Drupal core

Drupal core 7.44 — Update available ⚠

Recommended version: 7.50 (2016-Jul-07)

- Download
- Release notes

Includes:

- Enabled: *Block, Comment, Contextual links, Field, Field SQL storage, Field UI, File, Filter, Help, Image, List, Menu, Node, Number, Options, Path, RDF, Search, Shortcut, Statistics, Syslog, System, Taxonomy, Text, Update manager, User*
- Disabled: *Aggregator, Bartik, Blog, Book, Color, Contact, Content translation, Dashboard, Database logging, Forum, Garland, Locale, OpenID, Overlay, PHP filter, Poll, Seven, Stark, Testing, Toolbar, Tracker, Trigger*

Modules

Acquia Connector 7.x-2.17 — Up to date ✓

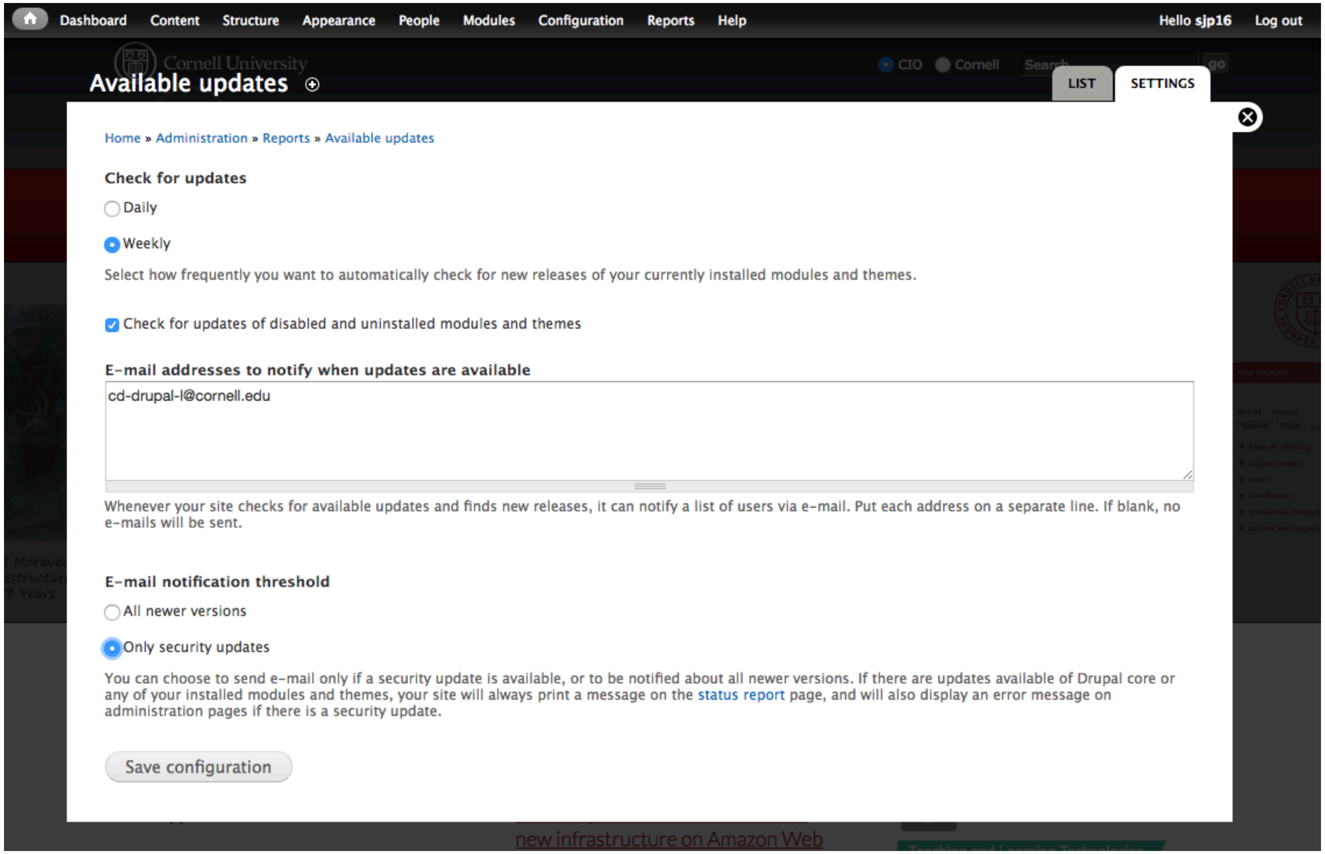
Also available: 7.x-3.0-alpha3 (2016-Aug-23)

- Download
- Release notes

Includes: *Acquia Site Profile Information, Acquia agent, Acquia search*

Site can send email to admins

- Options: daily/weekly, all updates/security only



Available updates

Home » Administration » Reports » Available updates

Check for updates

○ Daily

● Weekly

Select how frequently you want to automatically check for new releases of your currently installed modules and themes.

☑ Check for updates of disabled and uninstalled modules and themes

E-mail addresses to notify when updates are available

cd-drupal-l@cornell.edu

Whenever your site checks for available updates and finds new releases, it can notify a list of users via e-mail. Put each address on a separate line. If blank, no e-mails will be sent.

E-mail notification threshold

○ All newer versions

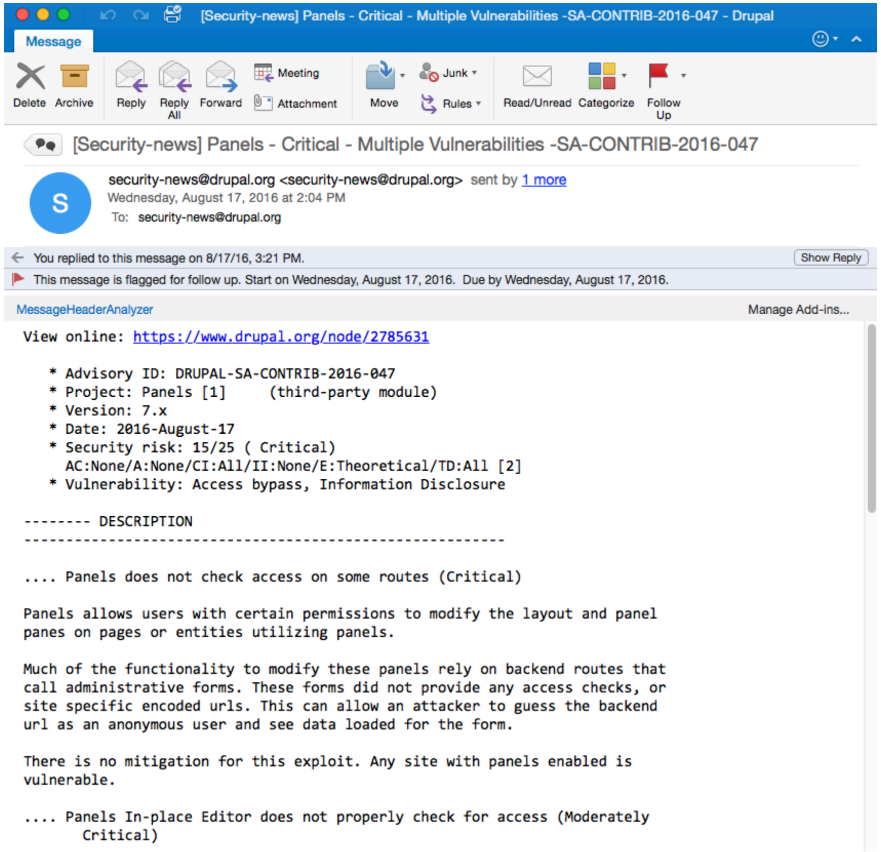
● Only security updates

You can choose to send e-mail only if a security update is available, or to be notified about all newer versions. If there are updates available of Drupal core or any of your installed modules and themes, your site will always print a message on the status report page, and will also display an error message on administration pages if there is a security update.

Save configuration

Security news from Drupal.org

- Sign up at drupal.org to receive security alerts



[Security-news] Panels - Critical - Multiple Vulnerabilities -SA-CONTRIB-2016-047

S

security-news@drupal.org <security-news@drupal.org> sent by 1 more
Wednesday, August 17, 2016 at 2:04 PM
To: security-news@drupal.org

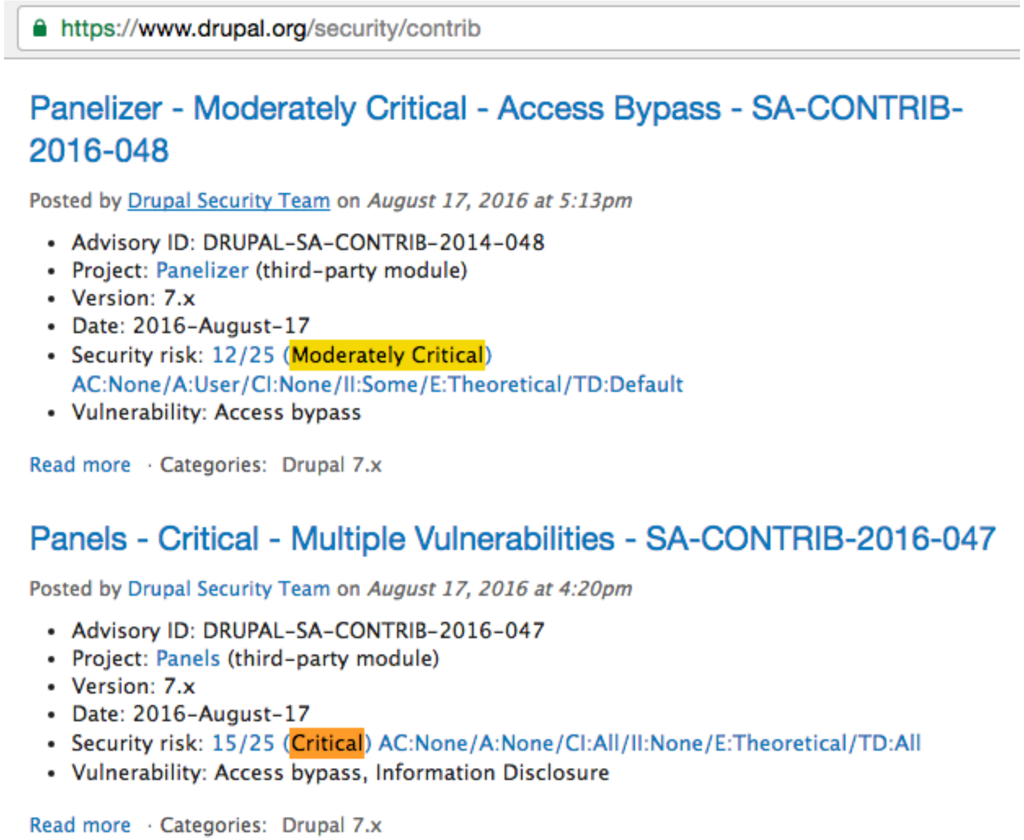
You replied to this message on 8/17/16, 3:21 PM.

This message is flagged for follow up. Start on Wednesday, August 17, 2016. Due by Wednesday, August 17, 2016.

```
View online: https://www.drupal.org/node/2785631

   * Advisory ID: DRUPAL-SA-CONTRIB-2016-047
   * Project: Panels [1]     (third-party module)
   * Version: 7.x
   * Date: 2016-August-17
   * Security risk: 15/25 ( Critical)
     AC:None/A:None/CI:All/II:None/E:Theoretical/TD:All [2]
   * Vulnerability: Access bypass, Information Disclosure

-------- DESCRIPTION
---------------------------------------------------------

.... Panels does not check access on some routes (Critical)

Panels allows users with certain permissions to modify the layout and panel
panes on pages or entities utilizing panels.

Much of the functionality to modify these panels rely on backend routes that
call administrative forms. These forms did not provide any access checks, or
site specific encoded urls. This can allow an attacker to guess the backend
url as an anonymous user and see data loaded for the form.

There is no mitigation for this exploit. Any site with panels enabled is
vulnerable.

.... Panels In-place Editor does not properly check for access (Moderately
       Critical)
```

Review announcement online

- Rating shows how critical each update is



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

Panelizer - Moderately Critical - Access Bypass - SA-CONTRIB-2016-048

Posted by Drupal Security Team on *August 17, 2016 at 5:13pm*

- Advisory ID: DRUPAL-SA-CONTRIB-2014-048
- Project: Panelizer (third-party module)
- Version: 7.x
- Date: 2016-August-17
- Security risk: 12/25 (Moderately Critical) AC:None/A:User/CI:None/II:Some/E:Theoretical/TD:Default
- Vulnerability: Access bypass

Read more · Categories: Drupal 7.x

Panels - Critical - Multiple Vulnerabilities - SA-CONTRIB-2016-047

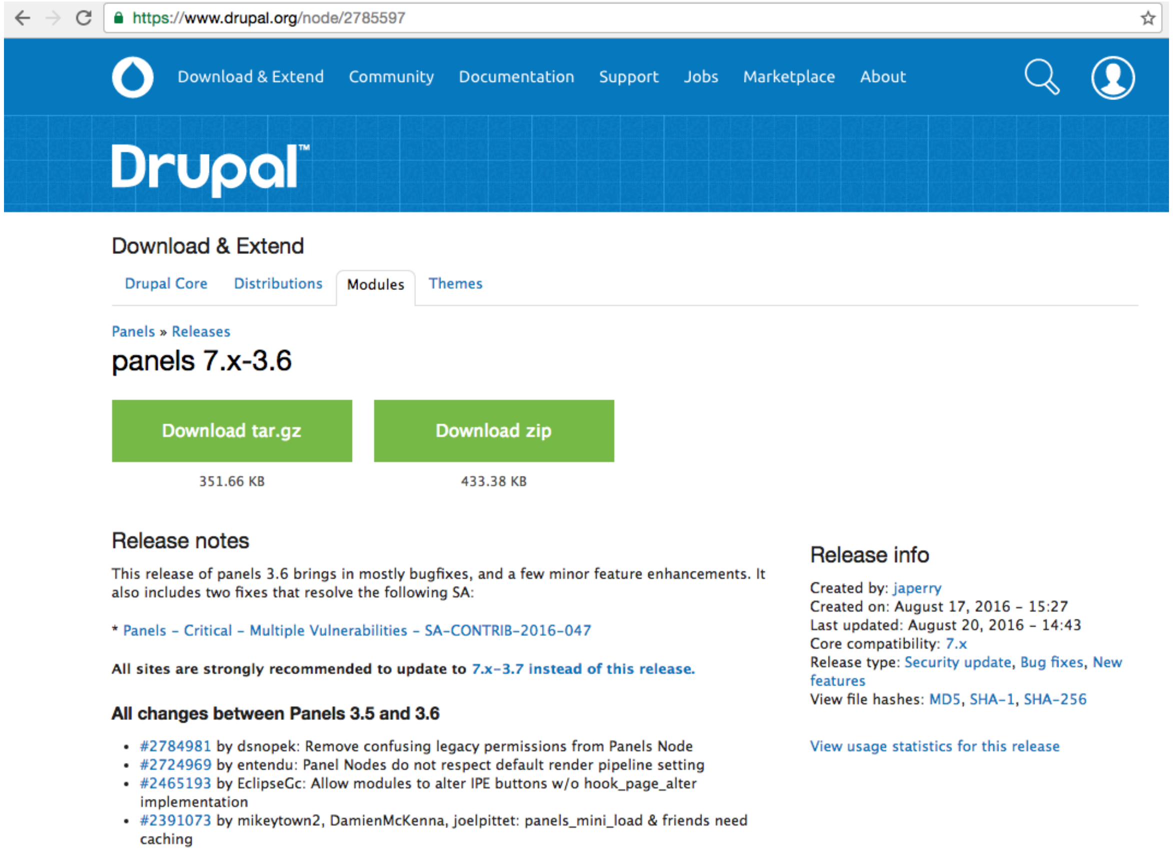
Posted by Drupal Security Team on *August 17, 2016 at 4:20pm*

- Advisory ID: DRUPAL-SA-CONTRIB-2016-047
- Project: Panels (third-party module)
- Version: 7.x
- Date: 2016-August-17
- Security risk: 15/25 (Critical) AC:None/A:None/CI:All/II:None/E:Theoretical/TD:All
- Vulnerability: Access bypass, Information Disclosure

Read more · Categories: Drupal 7.x

Review details of module update

- Notice a newer release may be recommended



Download & Extend

Drupal Core | Distributions | Modules | Themes

Panels » Releases

panels 7.x-3.6

Download tar.gz — 351.66 KB

Download zip — 433.38 KB

Release notes

This release of panels 3.6 brings in mostly bugfixes, and a few minor feature enhancements. It also includes two fixes that resolve the following SA:

* Panels - Critical - Multiple Vulnerabilities - SA-CONTRIB-2016-047

All sites are strongly recommended to update to 7.x-3.7 instead of this release.

All changes between Panels 3.5 and 3.6

- #2784981 by dsnopek: Remove confusing legacy permissions from Panels Node
- #2724969 by entendu: Panel Nodes do not respect default render pipeline setting
- #2465193 by EclipseGc: Allow modules to alter IPE buttons w/o hook_page_alter implementation
- #2391073 by mikeytown2, DamienMcKenna, joelpittet: panels_mini_load & friends need caching

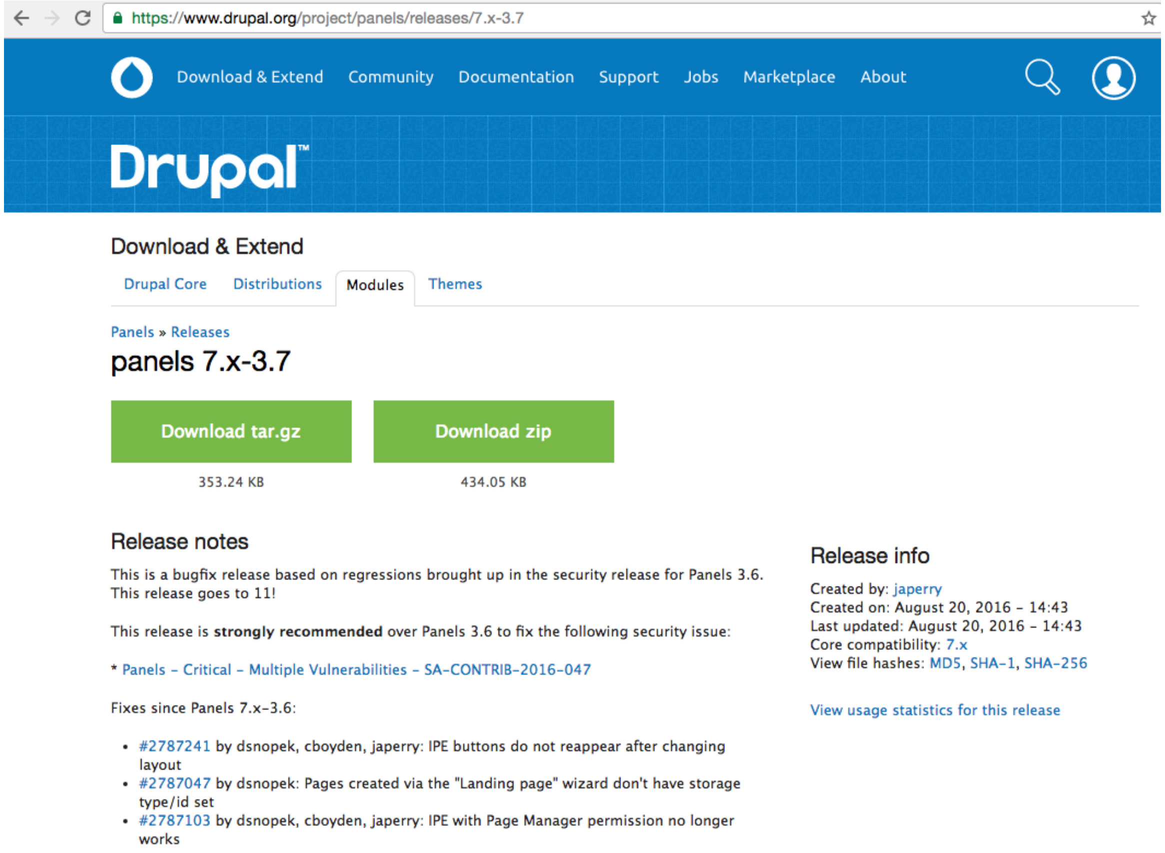
Release info

Created by: japerry
Created on: August 17, 2016 - 15:27
Last updated: August 20, 2016 - 14:43
Core compatibility: 7.x
Release type: Security update, Bug fixes, New features
View file hashes: MD5, SHA-1, SHA-256

View usage statistics for this release

Check newest release

- Review all releases newer than currently on site



Download & Extend

Panels » Releases

panels 7.x-3.7

353.24 KB

434.05 KB

Release notes

This is a bugfix release based on regressions brought up in the security release for Panels 3.6. This release goes to 11!

This release is **strongly recommended** over Panels 3.6 to fix the following security issue:

* Panels - Critical - Multiple Vulnerabilities - SA-CONTRIB-2016-047

Fixes since Panels 7.x-3.6:

- #2787241 by dsnopek, cboyden, japerry: IPE buttons do not reappear after changing layout
- #2787047 by dsnopek: Pages created via the "Landing page" wizard don't have storage type/id set
- #2787103 by dsnopek, cboyden, japerry: IPE with Page Manager permission no longer works

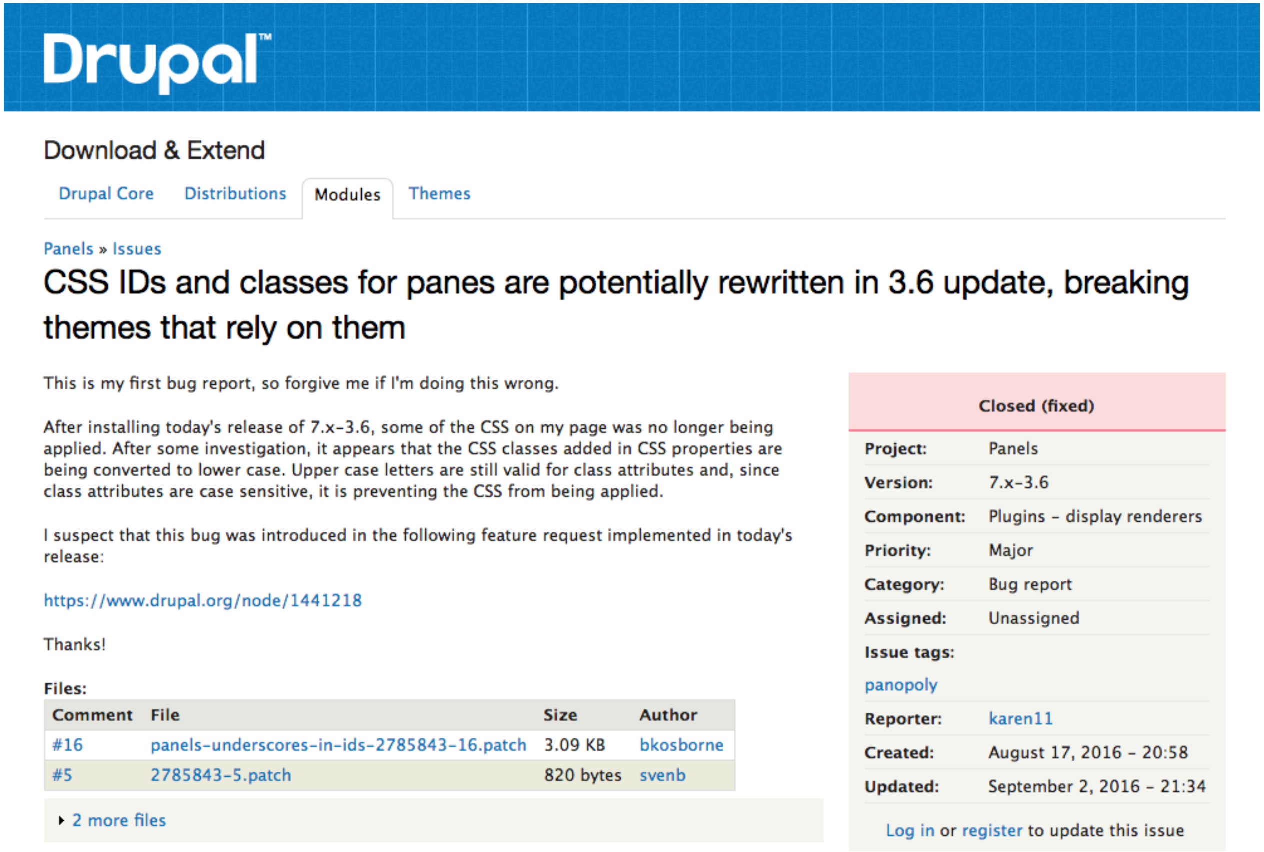
Release info

Created by: japerry
Created on: August 20, 2016 - 14:43
Last updated: August 20, 2016 - 14:43
Core compatibility: 7.x
View file hashes: MD5, SHA-1, SHA-256

View usage statistics for this release

Review each issue

- Does this specific change affect our site?



CSS IDs and classes for panes are potentially rewritten in 3.6 update, breaking themes that rely on them

This is my first bug report, so forgive me if I'm doing this wrong.

After installing today's release of 7.x-3.6, some of the CSS on my page was no longer being applied. After some investigation, it appears that the CSS classes added in CSS properties are being converted to lower case. Upper case letters are still valid for class attributes and, since class attributes are case sensitive, it is preventing the CSS from being applied.

I suspect that this bug was introduced in the following feature request implemented in today's release:

https://www.drupal.org/node/1441218

Thanks!

Files:

Comment	File	Size	Author
#16	panels-underscores-in-ids-2785843-16.patch	3.09 KB	bkosborne
#5	2785843-5.patch	820 bytes	svenb

▸ 2 more files

Closed (fixed)

Project:	Panels
Version:	7.x-3.6
Component:	Plugins - display renderers
Priority:	Major
Category:	Bug report
Assigned:	Unassigned
Issue tags:	
panopoly	
Reporter:	karen11
Created:	August 17, 2016 - 20:58
Updated:	September 2, 2016 - 21:34

Log in or register to update this issue

Drupal vendors can help

- A Drupal-centric vendor like Acquia or Pantheon can act quickly to block the most critical attacks
  - Sites are protected until a full update can be done
- Dashboard tools make updates easier
- Shared maintenance: time spent reviewing updates can be split among multiple sites

Steps to update a Drupal module

- Back up the site’s code and database
  - Make sure you can restore both if needed
- Download the new version
- Check whether the currently installed version has any patches that need to be kept
- Copy new version into the site’s code
- Push onto dev or test site
- Test everything
  - Updates may interact with other modules

Our process

- Review updates
- Install on development site
- Test
  - Specific issues described in release announcement
  - Site in general: look for interaction with other modules
- Copy to test site
- Ask site owner to test

Questions?

- Thanks for coming! Remember to update!