mediacurrent

Taking charge of the unknowns

The Project Management of a Drupalgeddon compromise

By: Brad MacDonald

July 24th, 2015

mediacurrent

Brad MacDonald

Sr Project Manager

@bjmac

mediacurrent

Today's Outline

- What this is about
- The "Uh-oh" moment
- The client, the strategy and plan of attack
- Mitigation
- Exceptions
- Questions


@Mediacurrent

mediacurrent

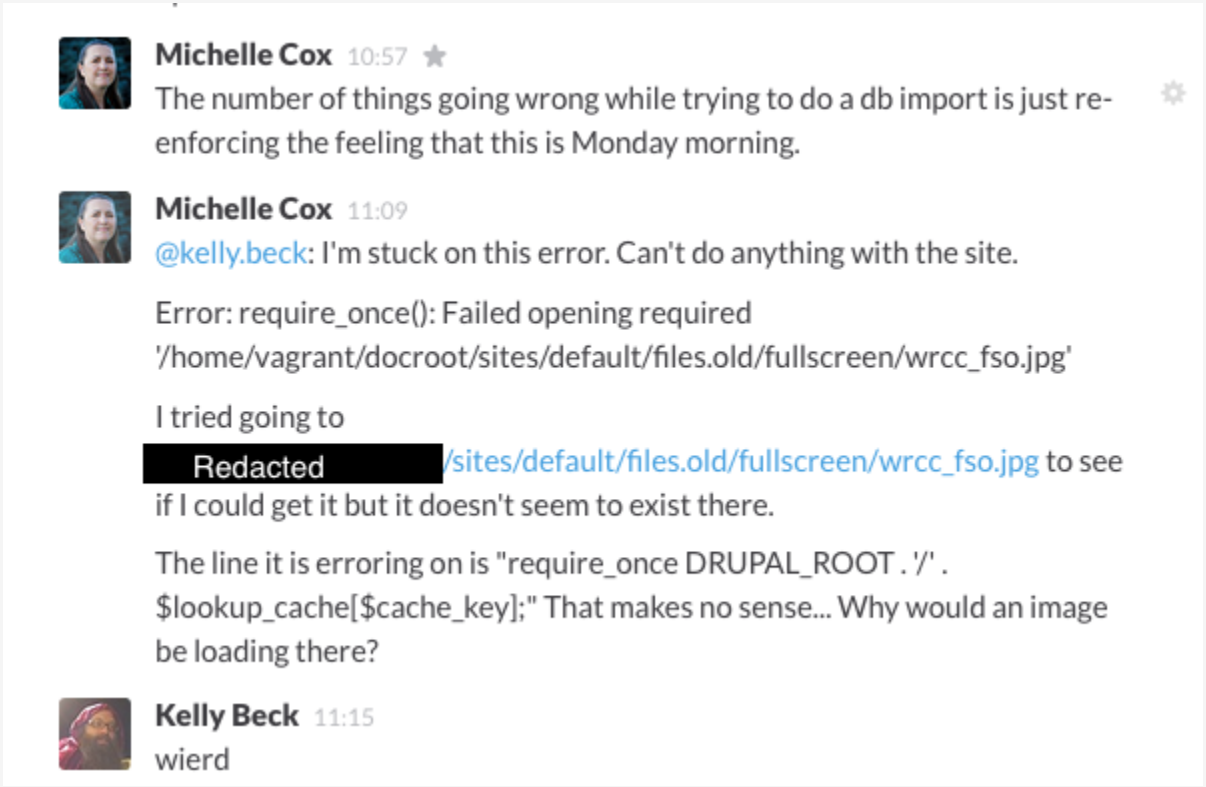
What is Drupalgeddon?

Why should I care?

A vulnerability in this API allows an attacker to send specially crafted requests resulting in arbitrary SQL execution. . .

@Mediacurrent

Bad news . . .



Michelle Cox 10:57

The number of things going wrong while trying to do a db import is just re-enforcing the feeling that this is Monday morning.

Michelle Cox 11:09

@kelly.beck: I'm stuck on this error. Can't do anything with the site.

Error: require_once(): Failed opening required '/home/vagrant/docroot/sites/default/files.old/fullscreen/wrcc_fso.jpg'

I tried going to [Redacted]/sites/default/files.old/fullscreen/wrcc_fso.jpg to see if I could get it but it doesn't seem to exist there.

The line it is erroring on is "require_once DRUPAL_ROOT . '/' . $lookup_cache[$cache_key];" That makes no sense... Why would an image be loading there?

Kelly Beck 11:15

wierd

mediacurrent

- Visitor on IP 27.16.99.2 checked the CHANGELOG.txt file and attempted to login several times; the first attempt was at 9:10pm on November 2nd.
- At 3:57:25am on November 3rd the visitor successfully logged in as user 1609; this is known because the visitor first loaded "user/login", submitted the login form via a POST call to the same page, and then loaded the "user/1609" page - this is Drupal's standard login procedure.
- The visitor did nothing for several hours
- At 8:47pm the visitor loaded the text formats page (GET /admin/config/content/formats) to see what text formats were configured.
- Immediately afterwards, the visitor loaded the "Add text format" page (GET /admin/config/content/formats/add) to create a new text format, then submitted the form (POST /admin/config/content/formats/add), creating the new "php_code" text filter.
- The visitor then went to the main "admin" page, and then to "admin/content" to see what content was on the site.
- The visitor then went to "node/add" and loaded up "node/add/page".
- The visitor submitted the "Create new page" page (POST /node/add/page) at 8:50pm, 8:51pm, 8:52pm and 8:54pm; at neither time did the visitor save the new node, indicating that they were pressing the "Preview" button in order to execute PHP code, without saving any data.

Uh-oh!

Communicating to the client the right way

@Mediacurrent


Whaaaaaaaat?

mediacurrent

PLANNING and STRATEGY
BEAT
uncertainty!

@Mediacurrent

mediacurrent

Security Team Assemble!

@Mediacurrent

mediacurrent

YOU CANNOT COMMUNICATE OR DOCUMENT ENOUGH!

@Mediacurrent

mediacurrent

All about the "W"s* a.k.a. the Strategy

- **W**hen it occurred?
- **W**here it came from?
- **W**hat was done?
- **H**ow it was accomplished?
- **W**hy it was done? (if possible)

* Yes there is an "H" in there

@Mediacurrent

What?

DrupalDefaultEntityController';

```
+-------------------------------+-------+-----------------------------------------------+--------+--------+
| name                          | type  | filename                                      | module | weight |
+-------------------------------+-------+-----------------------------------------------+--------+--------+
| DrupalDefaultEntityController | class | sites/default/files.old/fullscreen/wrcc_fso.jpg |      |      0 |
+-------------------------------+-------+-----------------------------------------------+--------+--------+
1 row in set (0.00 sec)

mysql> update registry set filename = 'includes/entity.inc' where name = 'DrupalDefaultEntityController';
Query OK, 1 row affected (0.00 sec)
Rows matched: 1  Changed: 1  Warnings: 0

mysql> select * from registry where name = 'DrupalDefaultEntityController';
+-------------------------------+-------+--------------------+--------+--------+
| name                          | type  | filename           | module | weight |
+-------------------------------+-------+--------------------+--------+--------+
| DrupalDefaultEntityController | class | includes/entity.inc |      |      0 |
+-------------------------------+-------+--------------------+--------+--------+
```

Where and when?

mediacurrent

How and Why

- We suspected all along it was Drupalgeddon, confirming was not as easy
- $$$$ is why

@Mediacurrent

mediacurrent

Mitigation

- Cleaned up the site and derivative data
- Removed the uploaded malware files
- Removing the malicious database registry entry
- Removed all accounts that are not verified
- Engage clients/stakeolders

@Mediacurrent

mediacurrent

Exceptions

mediacurrent

Thank You!

Questions?
@bjmac


@Mediacurrent


Mediacurrent.com


slideshare

slideshare.net/mediacurrent