



# Ramping up Security at an open-source startup

Lukas Reschke





whois `lukas@cloud.wtf`



**Delivers**

**SUBSCRIBE TODAY\***

\*Terms and Conditions apply

## Brunei needs cyber security personnel



CYBER threats and cyber security were the main topics of discussion this week in Las Vegas at Black Hat and Def Con, two of the world's largest gatherings for security professionals and hackers. Dan Geer, who

### ARTICLE TOOLS

Print this article

Email this article

Share this on: Adjust font size:

Twitter

Facebook



CONNECT TO THE BRUNEI TIMES



Like Share 30k

**BOOKMARKS**  
What's Hot

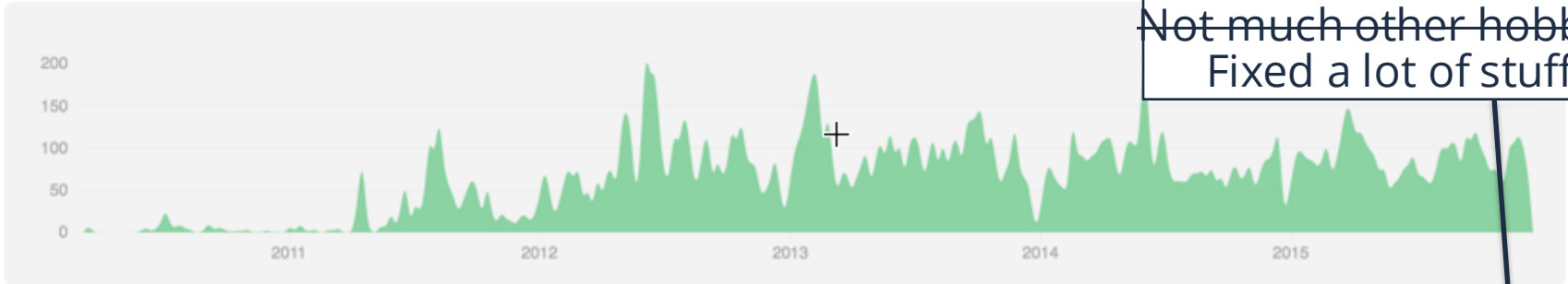
Behind the  
**headlines**

- Contributors
- Traffic
- Commits
- Code frequency
- Punch card
- Network
- Members

Mar 7, 2010 – Dec 20, 2015

Contributions: Commits

Contributions to master, excluding merge commits



Not much other hobbies  
Fixed a lot of stuff



Contributor since 2012



Employed since 2014





# The good and bad of the cloud



# Awesomeness of the cloud



- Accessible everywhere
- Back up online
- Easy sharing and collaboration
- All free!!!  
(or super cheap ... at least the licenses)

**There is NO CLOUD, just**



**other people's computers**



# Take back your data



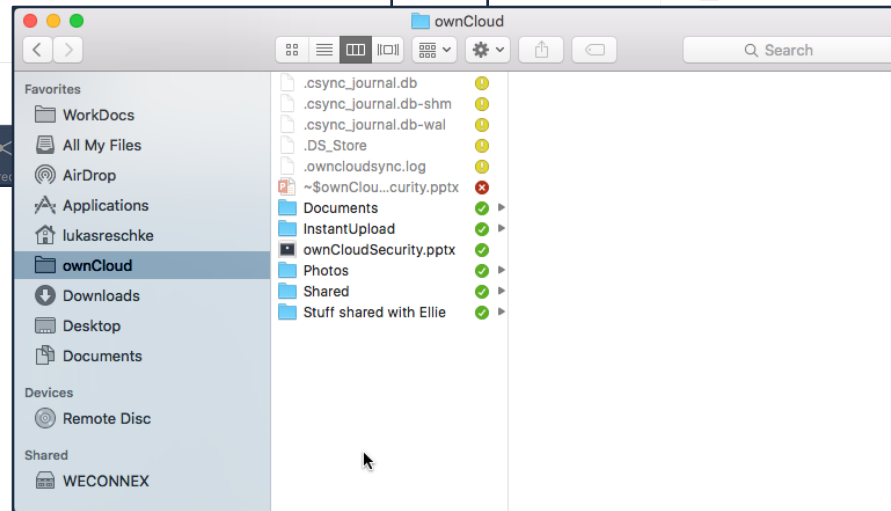
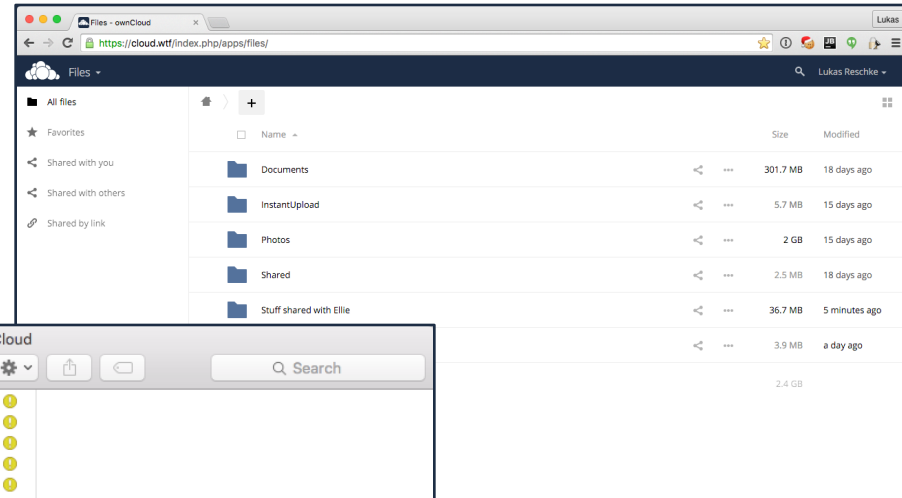
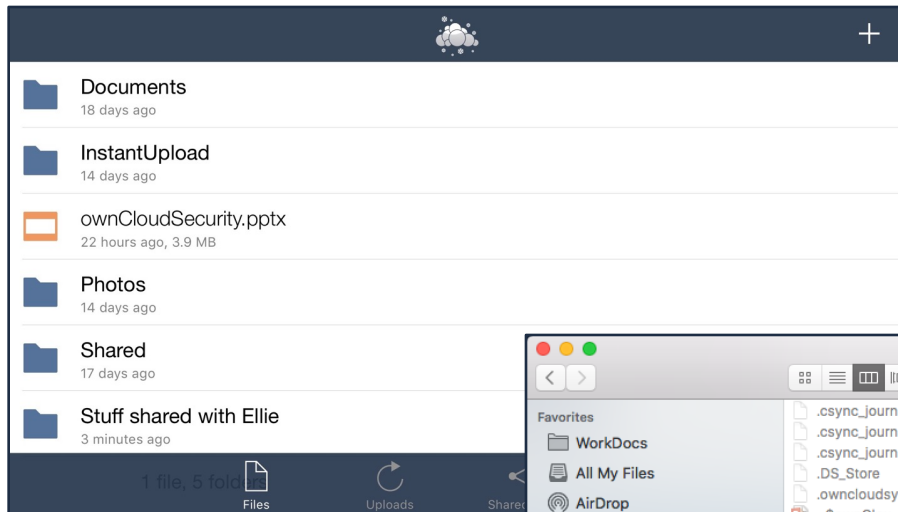
# Introducing ownCloud



- Sync and share
- Open Source
- Easy to use
- Easy to install
- Easy to extend
- > 8 million users



# Web / Desktop / Mobile





But that's not how we started...



mjob  Files Log Settings Admin Panel Logout

Home 

Upload file:  Keine ausgewählt

New  

 Selected



Hint: Mount it via webdav like this: <webdav://localhost:8088/webdav/owncloud.php>

# ... the project grew



[Project Overview](#) / [SCM overview](#) / [Activity by contributors](#)

Filtered by repository: All repositories ▾



Last 30 days

Last 365 days

Complete history

#	Authors	Commits	#	Authors	Commits	#	Authors	Commits
1	<a href="#">Thomas Müller</a>	592	1	<a href="#">Thomas Müller</a>	3053	1	<a href="#">Thomas Müller</a>	7307
2	<a href="#">Robin Appelman</a>	252	2	<a href="#">Morris Jobke</a>	1862	2	<a href="#">Thomas Tanghus</a>	6576
3	<a href="#">Roeland Douma</a>	210	3	<a href="#">Carla Schroder</a>	1722	3	<a href="#">Robin Appelman</a>	6197
4	<a href="#">Vincent Petry</a>	198	4	<a href="#">Joas Schilling</a>	1675	4	<a href="#">Bernhard Posselt</a>	5205
5	<a href="#">Carla Schroder</a>	155	5	<a href="#">Robin Appelman</a>	1470	5	<a href="#">Georg Ehrke</a>	4001
6	<a href="#">Joas Schilling</a>	125	6	<a href="#">Lukas Reschke</a>	1349	6	<a href="#">Morris Jobke</a>	3516
7	<a href="#">Morris Jobke</a>	125	7	<a href="#">Vincent Petry</a>	1324	7	<a href="#">Lukas Reschke</a>	3500
8	<a href="#">Jos Poortvliet</a>	121	8	<a href="#">Jos Poortvliet</a>	1001	8	<a href="#">Klaas Freitag</a>	3189
9	<a href="#">Lukas Reschke</a>	113	9	<a href="#">Olivier Paroz</a>	1001	9	<a href="#">Vincent Petry</a>	3050
10	<a href="#">Arthur Schiesser</a>	106	10	<a href="#">Roeland Douma</a>	999	10	<a href="#">Riemer Schipper</a>	2949

# ... and companies started to use it



# ... market leader in education + research



# Security at the start

- Everybody could push directly
- No formal code review process
- No static source code analysis
- No manual security testing
- No dedicated security personnel

(i.e. the same as still today in many companies ;-))



# Ensuring ownCloud Security



- Pull Request reviews

# Validate storage backend and auth mechanism before mounting #19313

**Open** Xenopathic wants to merge 2 commits into master from ext-validate-mount

Conversation 2 Commits 2 Files changed 15 +143 -40



Xenopathic commented 5 hours ago Collaborator

When an admin disables a backend for user mounting, any already created personal storages should no longer be mounted for the user.

Fixes #19312

cc @PVince81 @DeepDiver1975 @icewind1991

- Xenopathic added some commits 5 hours ago
  - Perform visibility checks on storages ... 2404333
  - Unit tests for storage validation in service ✓ 97c4691
- Xenopathic added **bug** **3 - To Review** **app:files\_external** **regression** labels 5 hours ago
- Xenopathic added this to the **8.2-current** milestone 5 hours ago



PVince81 commented 4 hours ago Collaborator

👍 works

I also tested regiving the permission and the storages were back.

**Labels**

- 3 - To Review
- app:files\_external
- bug
- regression

**Milestone**

- 8.2-current

**Assignee**

No one assigned

**3 participants**

Navigation sidebar with icons for code view, help, repository, and other actions.

"Ask programmers to review  
**10 lines of code**, they'll find  
**10 issues**.

Ask them to do **500 lines**  
and they'll say **it looks**  
**good**".

*The harsh truth about code reviews.*

# Ensuring ownCloud Security



- Pull Request reviews
- Regular code reviews for security issues

As a result of the security check conducted in September multiple critical vulnerabilities have been found, including:

1. Arbitrary local file disclosure via the office document conversion component. (similar to the issue found in the previews module)
2. Multiple XSS vulnerabilities
3. The documents application allows unauthenticated user to edit any public shared file
4. Bypass of the password protection
5. Allows logged-in users to access files of other users
6. A JSON injection

Furthermore, the SQL query in `op.php` is vulnerable against SQL injections if called with user-supplied parameters:

```
protected function hasOp($esId, $memberId, $opType){
    $ops = $this->execute(
        'SELECT * FROM ' . $this->tableName . ' WHERE `es_id`=? AND `opspec` LI
        array($esId)
    );
    $result = $ops->fetchAll();
    return is_array($result) && count($result)>0;
}
```

## Acceptance criteria

Criteria	Risk	Status	Verified	ID
The application <b>MUST</b> verify whether the user has all required privileges to access or modify the file.	High	X	7.0.2	1
The application <b>MUST NOT</b> leak any local files	High	~	7.0.2	2

- [Apps](#)
  - [Documents](#)

Clone this wiki locally

<https://github.com/owncloud/si>



Clone in Desktop

# Ensuring ownCloud Security



- Pull Request reviews
- Regular code reviews for security issues
- Automated static analysis



# Application: OwnCloud

Scan: Static: 20 Jul 2015 Static - a... | Dynamic

Request Readout

Max

Source Code View : *class.phpmailer.php*

Lines 1832-3418

Show:  Fix First Analyzer  Source Code Viewer  None

Load Different File

Goto Line

Source History...

```

2828 public function fixEOL($str)
2829 {
2830     // Normalise to \n
2831     $nstr = str_replace(array("\r\n", "\r"), "\n", $str);
2832     // Now convert LE as needed
2833     if ($this->LE !== "\n") {
2834         $nstr = str_replace("\n", $this->LE, $nstr);
2835     }
2836     return $nstr;
2837 }
2838
2839 /**
2840  * Add a custom header.
2841  * $name value can be overloaded to contain

```

High

Flaw ID: 849 Severity: High Type: loperator\_phpinclude Source: vobjectvalidate.php (line 15)  
 CWE ID: 98 Exploitability: Likely Category: Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion')

Viewing data path beginning in:

PHP files within owncloud-8.0.5-ee.zip (47)  
 owncloud/3rdparty/phpmailer/phpmailer/class.phpmail  
 fixEOL, line 2831

Data Path	Source			
	Filename/Class	Function Name	Line Number	Percent ?
End > 47	class.phpmailer.php	fixEOL	2831	
	46 class.phpmailer.php	wrapText	1481	
	45 class.phpmailer.php	setWordWrap	1612	
	44 phpmailerTest.php	buildBody	211	
	43 share.php	put	1901	
	42 share.php	shareItem	761	

Flaws

Data Path

# Ensuring ownCloud Security



- Pull Request reviews
- Regular code reviews for security issues
- Automated static analysis
- Customers do perform security tests
- Following industry best practice for security handling (oriented towards ISO 29147, 30111 and 27304)



# Security Advisory

[Back to advisories](#)

ownCloud server 8.1.2

[Command injection when using external SMB storage](#)

[PHP arbitrary class instantiation in "files\\_external"](#)

ownCloud desktop 2.0.1

[Improper validation of certificates when using self-signed certificates](#)

ownCloud mobile iOS 3.4.4

[Improper validation of certificates within the iOS application](#)

[Credentials potentially leaked to other configured ownCloud instance](#)

## PHP arbitrary class instantiation in "files\_external" (oC-SA-2015-018)

30th September 2015

Risk level: **High**

CVSS v2 Base Score: 9 (AV:N/AC:L/Au:S/C:C/I:C/A:C)

CWE: Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection') (CWE-470)

### Description

A user may instantiate arbitrary ownCloud classes due to a lack of a proper check of the mount point options provided by a user via the web front end. These may include constructor arguments and could potentially lead to a remote code execution.

### Affected Software

- ownCloud Server < **8.1.2** (CVE-2015-7699)
  - [core/a1706f61aaf822aeba4ea9e84b53c5cea984f8e4](#)
- ownCloud Server < **8.0.7** (CVE-2015-7699)
  - [core/595381b9bd5676492ff8957de0590982ed1864a4](#)
- ownCloud Server < **7.0.9** (CVE-2015-7699)
  - [core/b05e178bbf884b120d1106e6a28f35aa50d6d06f](#)

### Action Taken

The mount points are now properly validated in the controller before being stored.

### Acknowledgements

The ownCloud team thanks the following people for their research and responsible disclosure of the above advisory:

- Robin McCorkell - ownCloud Inc. (rmccorkell@owncloud.com) - Vulnerability discovery and disclosure.

Title

Risk

Common Weakness Enumeration

Vulnerability description

Affected software + patches + CVE

What we did to fix it

Credits



# Security work going on in ownCloud

May 26, 2015

Besides a lot of the [performance work](#) that was lately done as well as the [stability and architectural improvements](#) we work on, we are also striving to make ownCloud even more secure by improving our API as well as introducing new hardening features. In this blog post I am going to feature some of these changes.

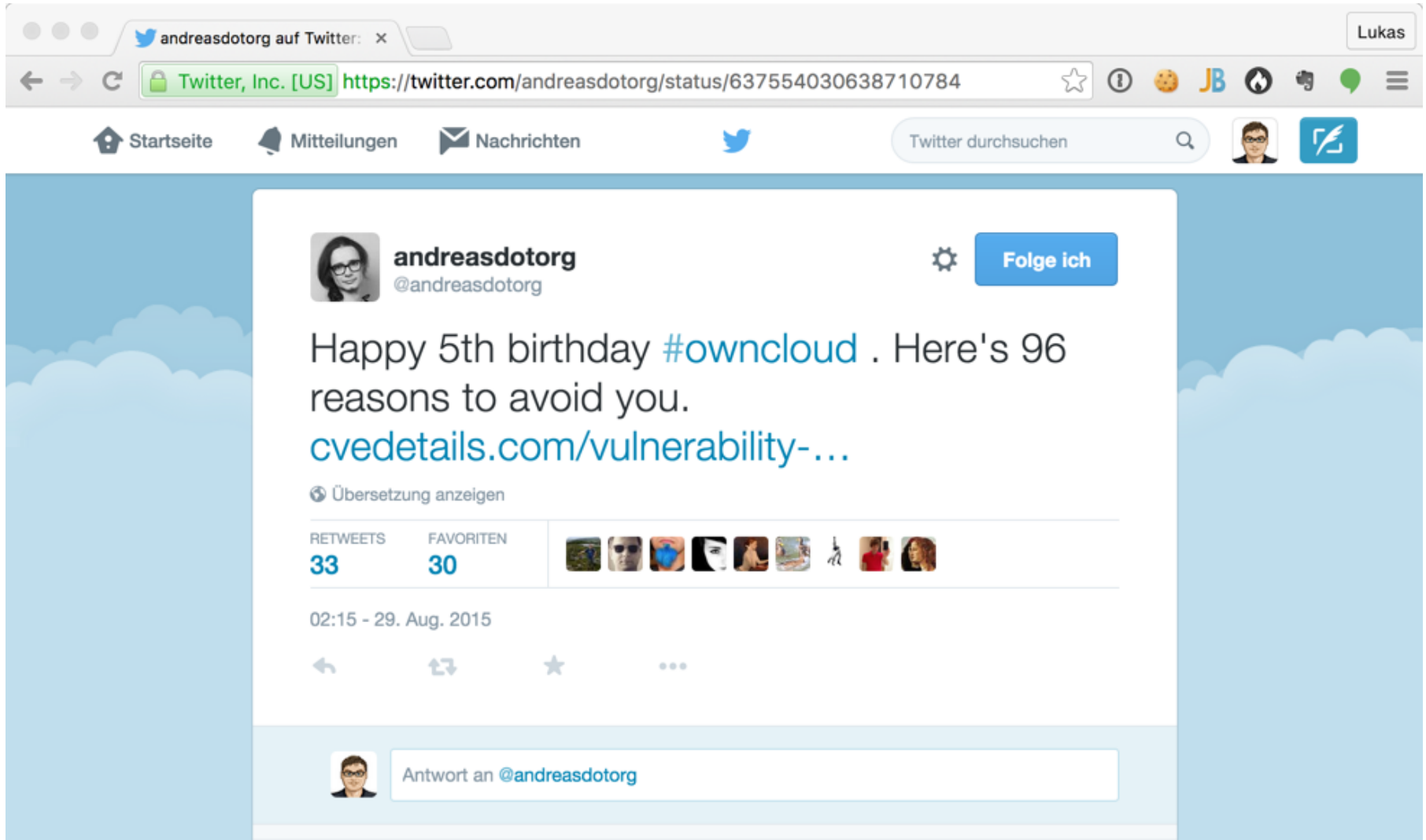
Those include:

- ["data/.htaccess" is updated after each update](#)
- [SabreDAV web interface has been removed](#)
- [Trusted domains are now a hard requirement](#)
- [Failed login log entries supports reverse proxy settings](#)
- [Request ID supports mod\\_unique\\_id](#)
- ["From link" download functionality has been removed](#)
- [Security-related headers can now be sent by the web server](#)
- [Enhancement of root certificate handling](#)
- [OC\\_User\\_HTTP backend replaced by user\\_webdavauth](#)
- [Random-number generator returns all base64 characters](#)
- [OC.generateUrl encodes parameters now automatically](#)
- [Code checker checks for strict comparisons in PHP code](#)
- [Constructor of OC\Files\View prevents directory traversals](#)
- [Stricter Content-Security-Policy and more choices for developers](#)
- [New security guidance and tips & tricks](#)

And yet...



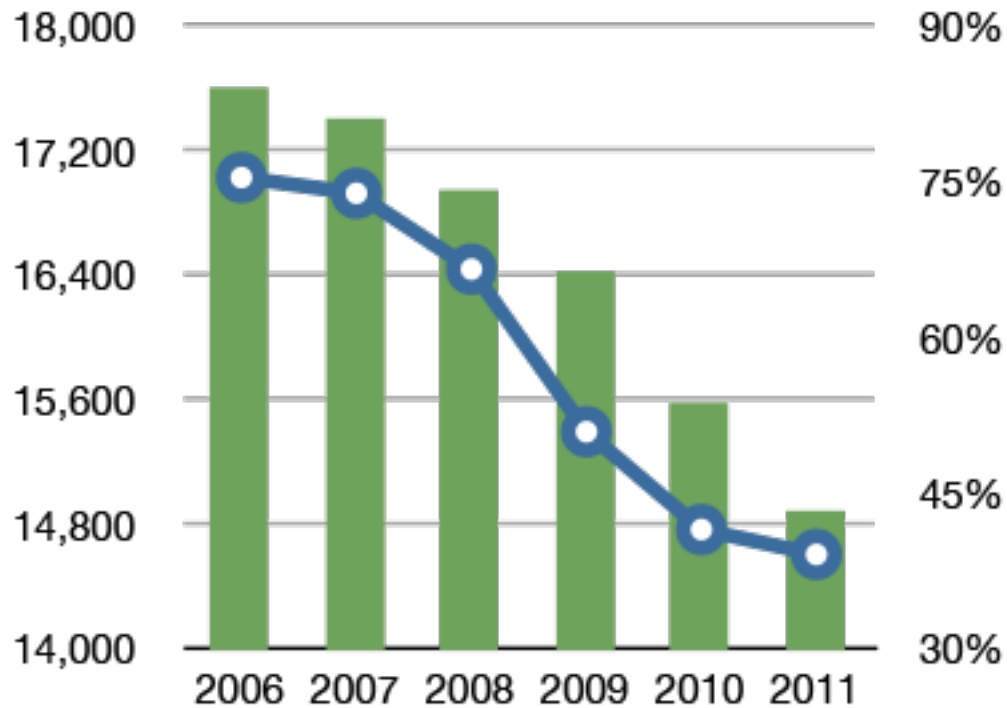
# And yet...



The screenshot shows a web browser window displaying a Twitter post. The browser's address bar shows the URL <https://twitter.com/andreasdotorg/status/637554030638710784>. The Twitter interface includes navigation icons for 'Startseite', 'Mitteilungen', and 'Nachrichten', along with a search bar and a user profile picture. The tweet is from the user 'andreasdotorg' (@andreasdotorg), who has a profile picture of a woman with glasses. The tweet text reads: 'Happy 5th birthday #owncloud . Here's 96 reasons to avoid you. [cvedetails.com/vulnerability-...](http://cvedetails.com/vulnerability-...)'. Below the text, there is a link to 'Übersetzung anzeigen'. The tweet has 33 retweets and 30 favorites, with a row of profile pictures of users who interacted with it. The timestamp is '02:15 - 29. Aug. 2015'. At the bottom, there is a reply box with the text 'Antwort an @andreasdotorg' and a small profile picture of the user 'Lukas'.

# How are we doing?

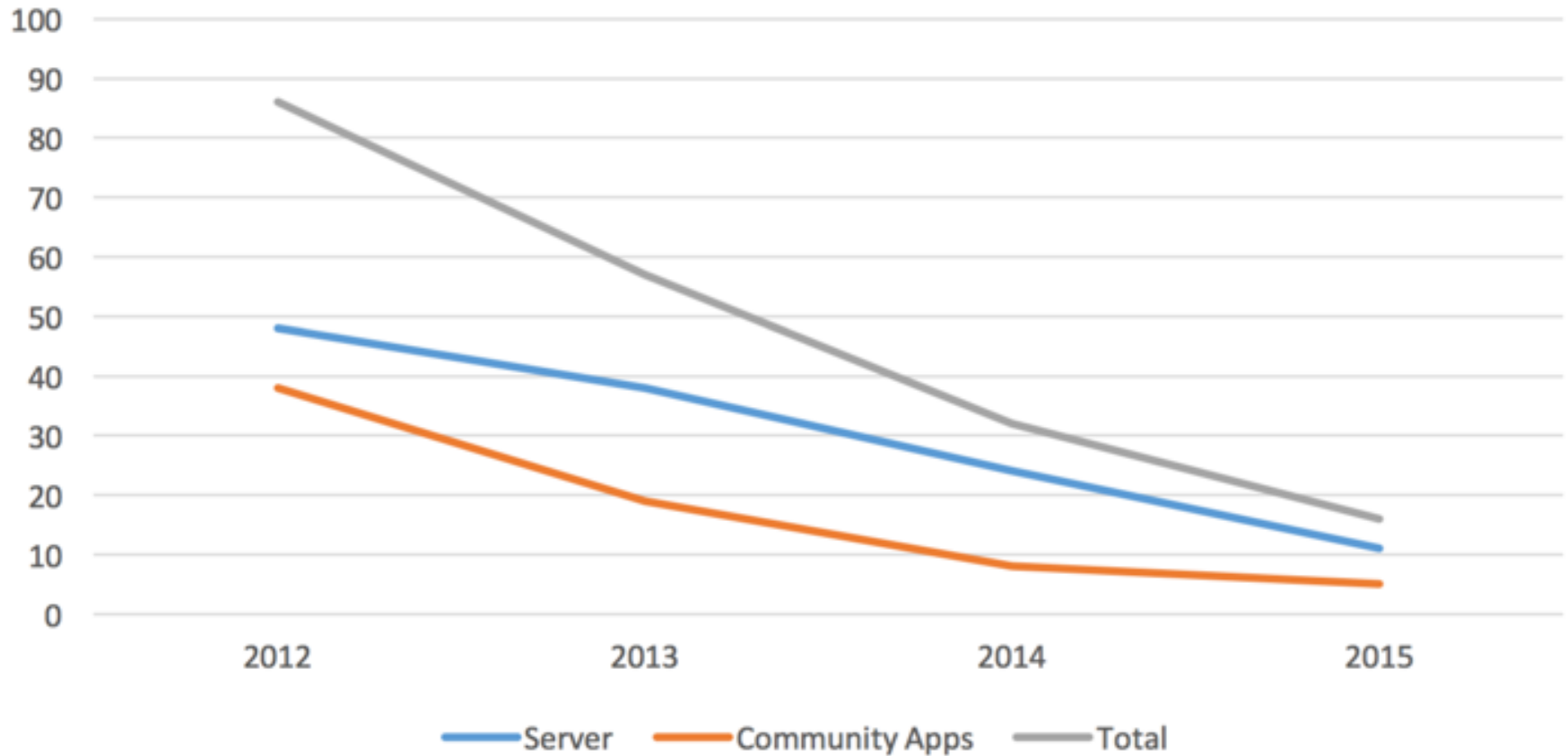
## Internet Explorer vs Murder Rate



 Murders in US       Internet Explorer Market Share

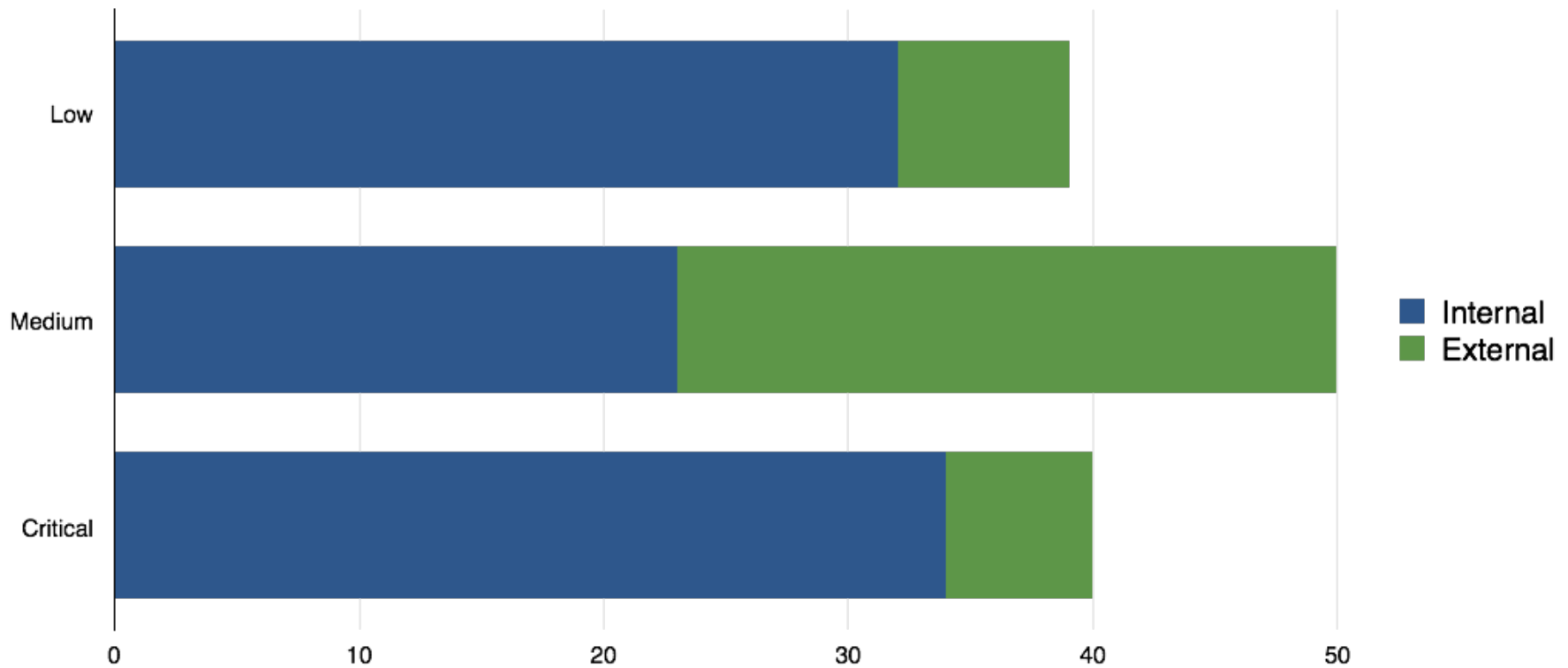
# How are we doing?

## Fixed vulnerabilities per year



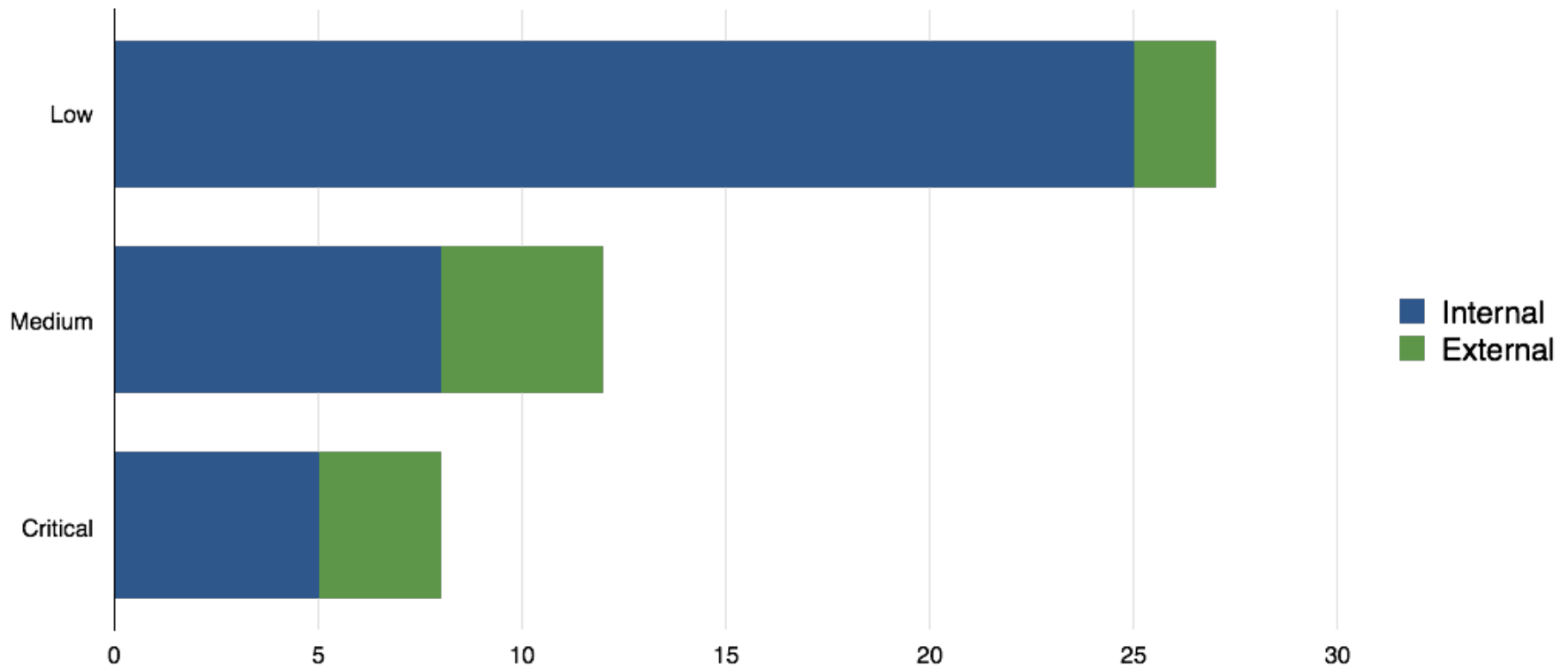
# How are we doing?

Severity by reporter in ownCloud Server since 2012



# How are we doing?

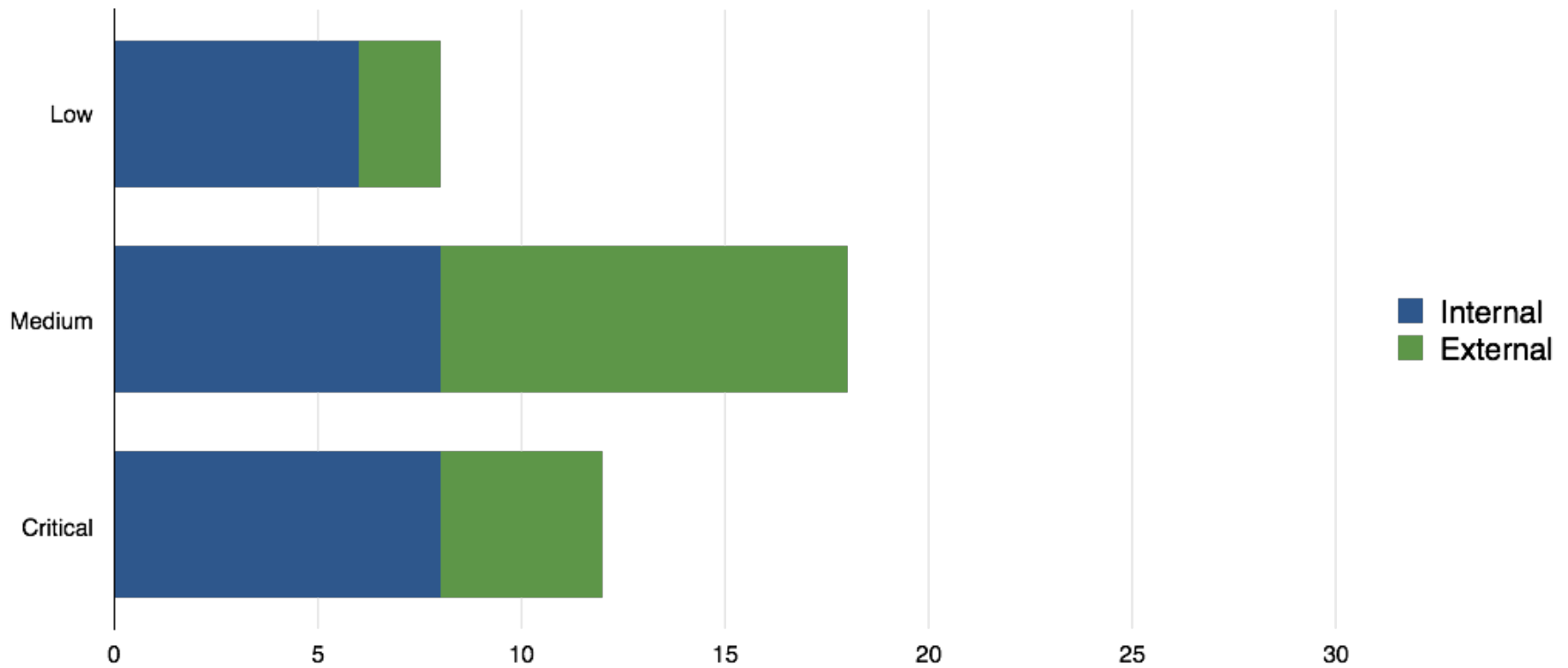
Severity by reporter in ownCloud Server in 2012





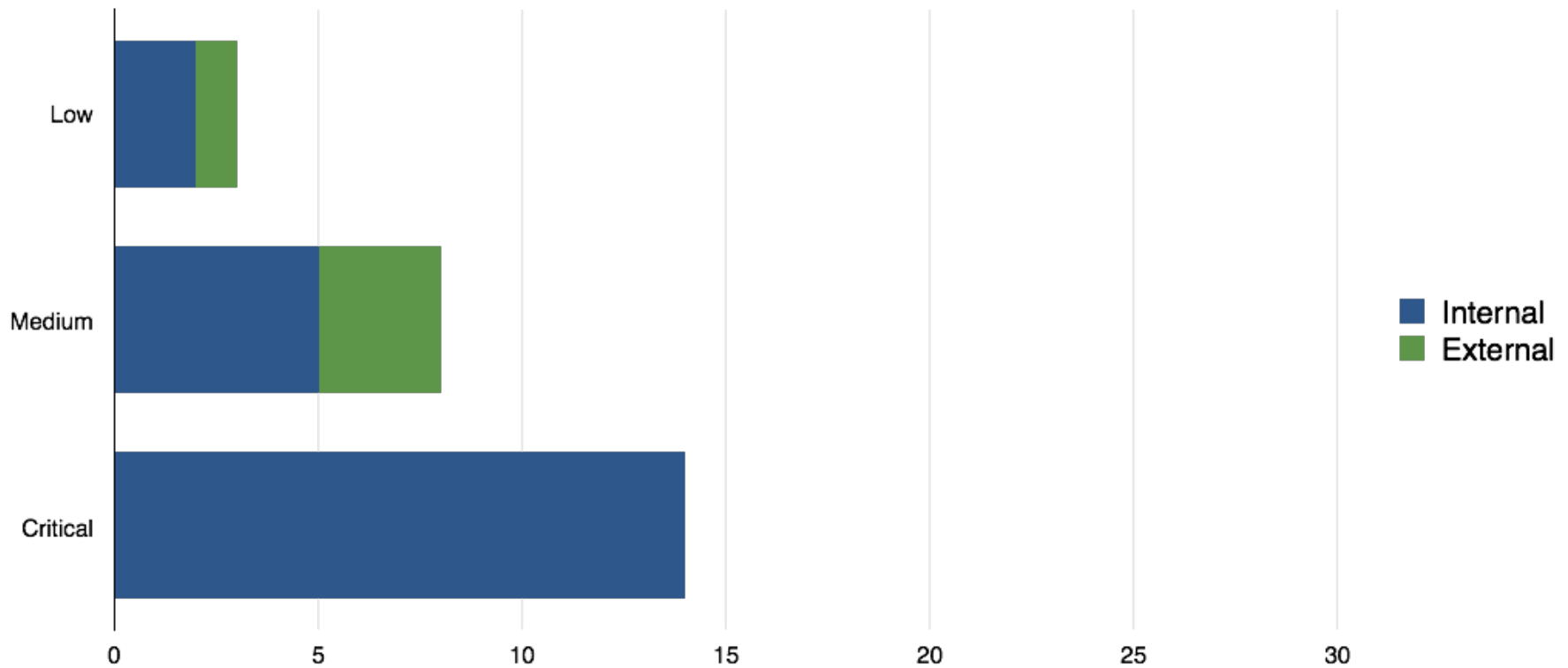
# How are we doing?

Severity by reporter in ownCloud Server in 2013



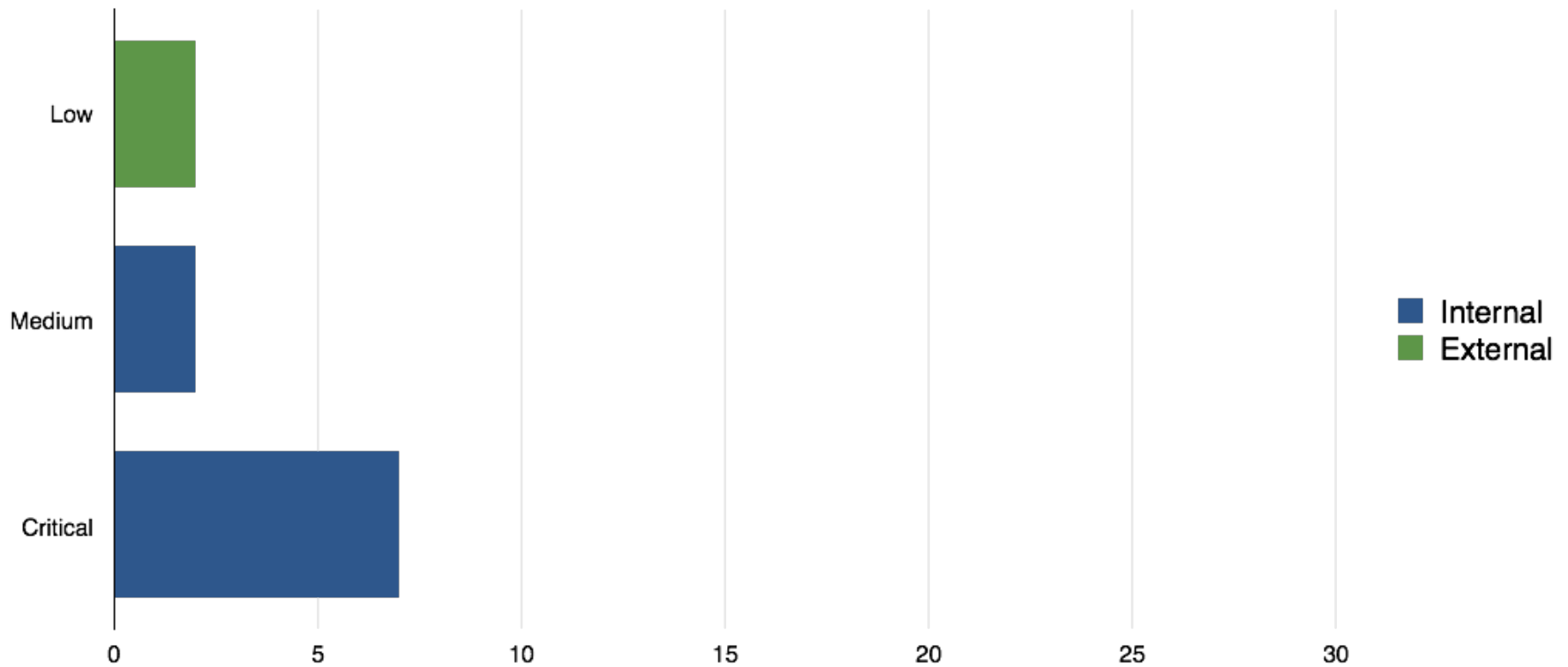
# How are we doing?

Severity by reporter in ownCloud Server in 2014



# How are we doing?

Severity by reporter in ownCloud Server in 2015



# Security: Secure by Default!

- Security checks have to be disabled by the developer (e.g. CSRF + authentication)

```
/**
 * @PublicPage ←
 * @NoCSRFRequired ←
 *
 * @param string $token
 * @param string $path
 * @return TemplateResponse|RedirectResponse
 * @throws NotFoundException
 */
public function showShare($token, $path = '') {
    \OC_User::setIncognitoMode(true);

    // Check whether share exists
    $linkItem = Share::getShareByToken($token, false);
    if($linkItem === false) {
        return new NotFoundResponse();
    }

    $shareOwner = $linkItem['uid_owner'];
    $originalSharePath = $this->getPath($token);

    // Share is password protected - check whether the user is permitted
    if (isset($linkItem['share_with']) && !Helper::authenticate($linkItem['share_with'], $token)) {
        return new RedirectResponse($this->urlGenerator->linkToRoute('file_index', array('token' => $token)));
    }

    if (Filesystem::isReadable($originalSharePath . $path)) {
        $getPath = Filesystem::normalizePath($path);
    }
}
```

# Security: Secure by Default!



- Security checks have to be disabled by the developer (e.g. CSRF + Authentication)
- Internal file system not vulnerable against directory traversal

```
/**
 * @param string $token
 * @param string $path
 * @return TemplateResponse|RedirectResponse
 * @throws NotFoundException
 */
public function accessFolder($token, $path = '') {
    // Ordner der gechrootet wird
    $view = new OC\Files\View('/folderToChroot/');
    // Funktioniert
    $view->fopen('myfile.txt', 'r');
    // Funktioniert NICHT
    $view->fopen('../../myfile.txt', 'r');
}
```

# Security: Secure by Default!



- Security checks have to be disabled by the developer (e.g. CSRF + Authentication)
- Internal file system not vulnerable against directory traversal
- Security functionalities are enabled by default in ownCloud server (e.g. Content-Security-Policy)
- ...



# Potential dangerous PHP functions are blacklisted

```
1. lukasreschke@Lukass-MBP: ~/Documents/Programming/master (zsh)
line 34: OC_Util - Static method of private class must not be called
Analysing /Users/lukasreschke/Documents/Programming/master/apps/not-compliant/download.php
5 errors
line 42: OC_Helper - Static method of private class must not be called
line 45: OCP\Response - Static method of deprecated class must not be called
line 46: OCP\Response - Static method of deprecated class must not be called
line 47: OCP\Response - Static method of deprecated class must not be called
line 49: OC_Util - Static method of private class must not be called
Analysing /Users/lukasreschke/Documents/Programming/master/apps/not-compliant/index.php
6 errors
line 61: OC_Util - Static method of private class must not be called
line 63: OCP\App::setActiveNavigationEntry - Method of deprecated class must not be called
line 82: OCP\Util::linkTo - Method of deprecated class must not be called
line 86: OC_User - Static method of private class must not be called
line 92: OC_Helper - Static method of private class must not be called
line 118: OC_App - Static method of private class must not be called
Analysing /Users/lukasreschke/Documents/Programming/master/apps/not-compliant/lib/helper.php
7 errors
line 45: OC_Helper - Static method of private class must not be called
line 46: OC_L10N - private class must not be instantiated
line 69: OC_Helper - Static method of private class must not be called
line 72: OC_Helper - Static method of private class must not be called
line 74: OC_Helper - Static method of private class must not be called
line 77: OC_Helper - Static method of private class must not be called
line 140: OCP\Util::formatDate - Method of deprecated class must not be called
Analysing /Users/lukasreschke/Documents/Programming/master/apps/not-compliant/templates/list.php
1 errors
line 94: OCP\Util::linkTo - Method of deprecated class must not be called
Deprecated field available: shipped => true
Deprecated field available: standalone
Migrate the app version to appinfo/info.xml (add <version>1.1.11</version> to appinfo/info.xml and remove appinfo/version)
App is not compliant
→ master git:(master) X
```

# Security is hard





# ownCloud

ownCloud, Inc. is the company behind the ownCloud Project - the most downloaded open source project for data and file sync, share and view.

[www.owncloud.com](http://www.owncloud.com) · [@ownCloud](https://twitter.com/ownCloud)

Profile

Thanks

Submit Report

No technology is perfect, and ownCloud Inc. believes that working with skilled security researchers across the globe is crucial in identifying weaknesses in any technology. We created the ownCloud Security Bug Bounty Program to reward security researchers for finding issues in the ownCloud Server, and in so doing help strengthen ownCloud Server for customers, users and the community. If the submitter chooses not to get a bounty, emailed to the ownCloud security mailing list ([security@owncloud.com](mailto:security@owncloud.com)).

For the time being we want to focus our efforts on ownCloud Server instead of vulnerabilities within our website or infrastructure. However, if you find a security bug in our website or infrastructure we welcome any report, though we cannot offer a monetary incentive. Please do read the defined scope below carefully.

DO NOT RUN AUTOMATED SCANNERS AGAINST \*.OWNCLOUD.COM AND \*.OWNCLOUD.ORG SERVERS. AUTOMATED SCANS AGAINST OUR INFRASTRUCTURE MAY BE MARKED AS NOT APPLICABLE.

If you have questions please direct them to [lukas@owncloud.com](mailto:lukas@owncloud.com)

## Rewards

If the bug is identified as meaningful and qualifies for the program, and the submitter has followed the Disclosure Policy, the bug bounty is paid out on the following schedule by bug severity:

Impact	Definition	Reward
Critical	Giving the adversary complete control over the server. (RCE / SQL Injection / ...)	\$250-\$500

\$25

Minimum bounty

20

Hackers thanked

21

Reports closed

## Top Hackers



**ishahriyar**  
Reputation: 37



**ashesh**  
Reputation: 30



**psych0tr1a**  
Reputation: 14



**mandeep**  
Reputation: 9



**00day**  
Reputation: 7

# Why HackerOne?

- Used by other major vendors



Yahoo!



Twitter



Adobe



Mail.Ru



Square



Snapchat



Airbnb



Slack



Dropbox

- Great triaging tools and support
- Payments processed by HackerOne

# The platform



1 Reports - HackerOne x Lukas

HackerOne, Inc. [US] [https://hackerone.com/bugs?subject=owncloud&report\\_id=89856&view=closed&substates%5B%5D=resolved&...](https://hackerone.com/bugs?subject=owncloud&report_id=89856&view=closed&substates%5B%5D=resolved&...)

Hacktivity Directory Reports Dashboard

Open (26) Closed (225) Search all reports

Show: 25 Sort: Latest activity Show filters

- #89856 SMTP Protection not used 24 hours ago Reporter: ahmedadel
- #84023 xss in <https://apps.owncloud.com> about 1 day ago Reporter: testalways
- #84147 Essential Exported Services On android app (com.owncloud.android) 5 days ago Reporter: deepak\_das
- #89213 URGENT Email forgery using mandrill app 6 days ago Reporter: naveedsheik
- #89097 owncloud.com: CVE-2015-5477 BIND9 TKEY Vulnerability + Exploit (Denial of Service) 6 days ago Reporter: 1n3
- #84581 owncloud.com: Outdated plugins contains public exploits 7 days ago Reporter: mandeep
- #83710 apps.owncloud.com: SSL Session cookie without secure flag set 7 days ago Reporter: ashesh Reference: 167

### #89856 SMTP Protection not used

[ADD SUMMARY](#)

TIMELINE

**ahmedadel** reported a bug to [ownCloud](#). show raw · Sep 21st

Hello ownCloud,

I'm checking your website found spf record there.

You should apply strict SMPT policy to stop spoofed email sending from your domain. An attacker would send a Fake email from [info@owncloud.com](mailto:info@owncloud.com) saying that Please change your password, The victim is aware of phishing attacks, But when he sees that the mail originated from [info@owncloud.com](mailto:info@owncloud.com), He has no other way than to believe it. Clicking on the link takes him to a website where certain JavaScript is executed which steals his owncloud.com id and password (SESSION COOKIE). The results can be more dangerous.

when I tried to send a email from [info@owncloud.com](mailto:info@owncloud.com) to my email ,it was successful but when i tried to send the another from [admin@facebook.com](mailto:admin@facebook.com) or any other , i did not receive any email. Hence, there might be some configuration missing in your mail servers

Fix :

Your SPF record is "v=spf1 mx include:\_spf.google.com a:kerio.owncloud.com a:m.hive01.com include:cmail1.com include:email.influitive.com ~all"

It should be "v=spf1 mx include:\_spf.google.com a:kerio.owncloud.com a:m.hive01.com include:cmail1.com include:email.influitive.com ~all"

State

- Duplicate (Closed)

Type

Missing Best Practice

Participants

[\(Add participant\)](#)

Notifications

Enabled

Duplicate Of

[#83253](#)

New

Triaged

Closed

Bugs are closed by the Response Team when they consider the issue to be fully resolved.

Public

# The platform



1 Reports - HackerOne

HackerOne, Inc. [US] [https://hackerone.com/bugs?subject=owncloud&report\\_id=89856&view=closed&substates%5B%5D=resolved&...](https://hackerone.com/bugs?subject=owncloud&report_id=89856&view=closed&substates%5B%5D=resolved&...)

Hacktivity Directory Reports Dashboard

Open (26) Closed (225) Search all reports

Show: 25 Sort: Latest activity Show filters

- #89856 SMTP Protection not used 24 hours ago  
Reporter: ahmedadel
- #84023 xss in <https://apps.owncloud.com> about 1 day ago  
Reporter: testalways
- #84147 Essential Exported Services On android app (com.owncloud.android) 5 days ago  
Reporter: deepak\_das
- #89213 URGENT Email forgery using mandrill app 6 days ago  
Reporter: naveedsheik
- #89097 owncloud.com: CVE-2015-5477 BIND9 TKEY Vulnerability + Exploit (Denial of Service) 6 days ago  
Reporter: 1n3
- #84581 owncloud.com: Outdated plugins contains public exploits 7 days ago  
Reporter: mandeep
- #83710 apps.owncloud.com: SSL Session cookie without secure flag set 7 days ago  
Reporter: ashesh • Reference: 167

**hackbot** posted an internal comment. Sep 21st (about 1 day ago)

Hey there! I am Hackbot, I help find possible duplicates and related reports. Here are my top suggestions:

- (82%) Report [#83253](#) (informative): SPF Protection not used, I can hijack your email server

I also found some public reports from other teams that are similar to this report:

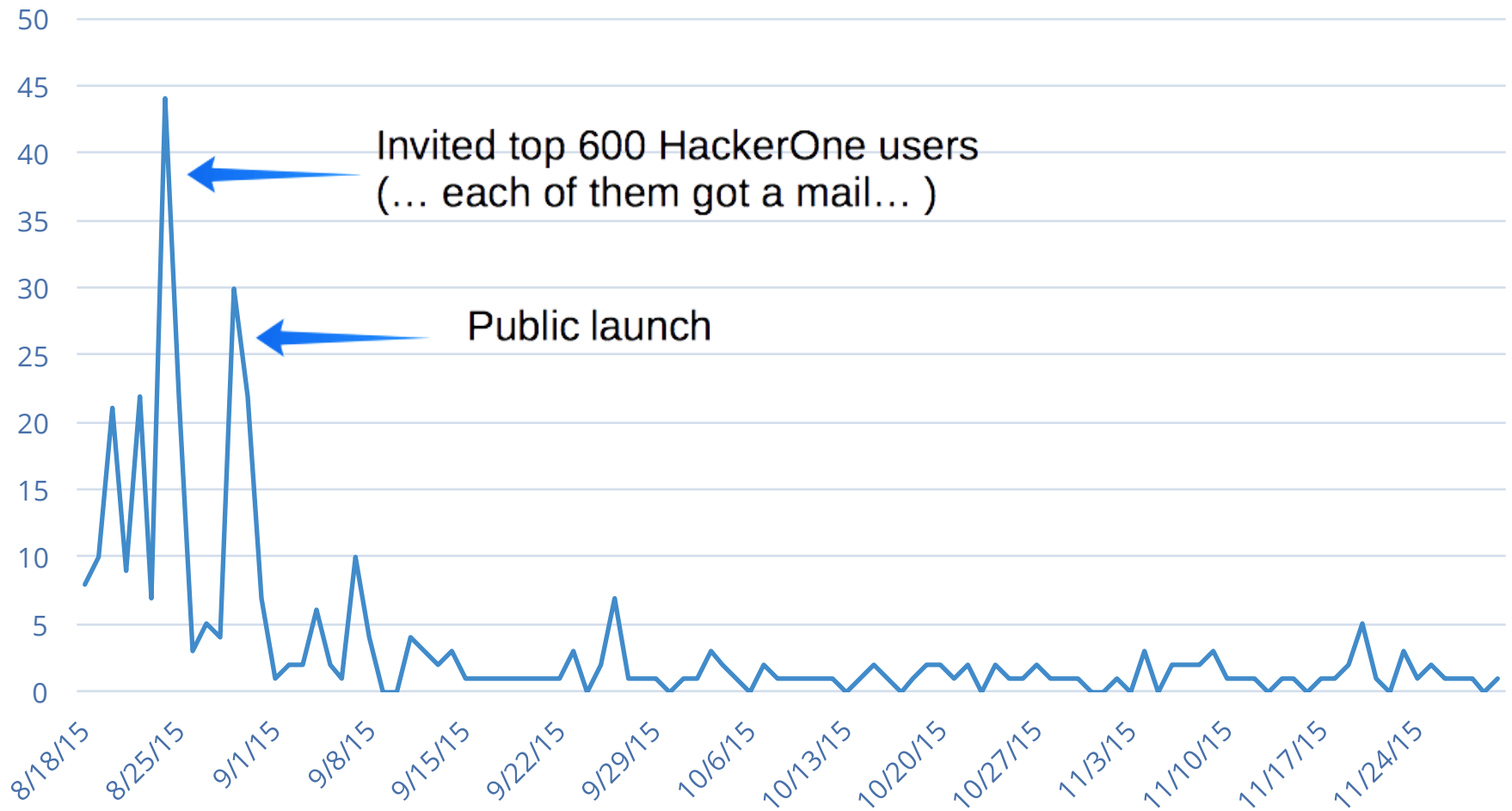
- (78%) Report [#77060](#) (resolved): SMTP protection not used
- (77%) Report [#56177](#) (resolved): SMTP protection not used
- (67%) Report [#25191](#) (informative): SMTP protection not used (please read carefully )
- (51%) Report [#57736](#) (resolved): Missing spf flags for hackerone.com
- (50%) Report [#34112](#) (resolved): SMPT Protection not used, I can hijack your email server.

**lukasreschke** closed the bug and changed the status to Duplicate ([#83253](#)). Sep 21st (24 hours ago)

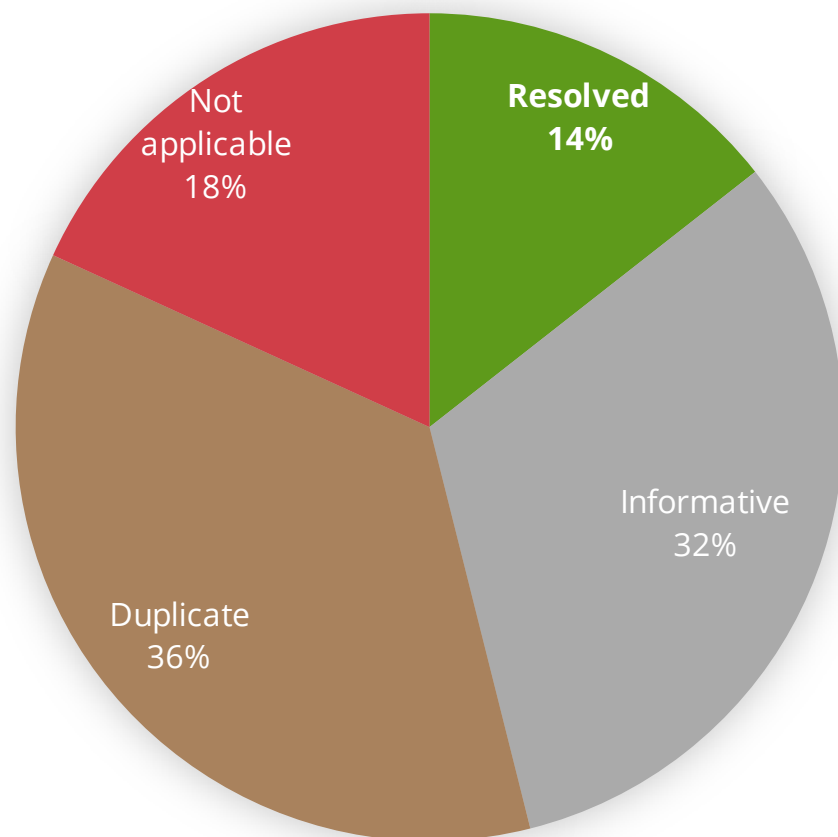
Thanks a lot for reporting this issue back to us. We do however have employed a policy using ~all on purpose since we're running mailing lists as well as other software on the same domain.

While we might consider to adjust this in the future for now we do consider this an acceptable behaviour and I will close this issue. See <http://serverfault.com/questions/611575/will-mailing-lists-break-if-spf-is-too-restrictive> for some considerations on problems with mailing lists and a too restrictive SPF policy.

# New Reports



## Type of reported bugs



## Resolved reports

- 3 bugs in scope (\$700)
- 43 bugs out of scope



# Lessons learned from a bug bounty program



- Protect infrastructure against automated testing tools in advance
  - Don't forget the contacts form
- Quality of reports differs hugely depending on the reporter
- Likely no low hanging fruits



What went wrong?  
What could have been better?

# Pull Request Reviews

- Added at a late stage.
- Prevents a lot of pitfalls
- ... ensure they actually get reviewed ...



The screenshot shows a web browser window with the URL `crypto.junod.info/2012/05/24/owncloud-4-0-and-encryption/`. The page title is "PASCAL JUNOD" and the subtitle is "A BILINGUAL BLOG ABOUT CRYPTOGRAPHY, INFORMATION SECURITY, SCIENCE, GEEKNESS AND OTHERS". The navigation menu includes "HOME", "IN A NUTSHELL", "PUBLICATIONS", "TEACHING", "PROFESSIONAL ACTIVITIES", and "CONTACT".

## OWNCLOUD 4.0 AND ENCRYPTION

24/05/2012 / PASCAL / 26 COMMENTS



Recently, the new version 4.0 of the OwnCloud open-source software has been released. According to Wikipedia, "OwnCloud is a software suite that provides a location-independent storage area for data (cloud storage). The project was launched in January 2010 from KDE developer Frank Karlitschek to create a free alternative to commercial cloud providers. In contrast to commercial storage services, ownCloud can be installed on a private server at no additional cost". So, anybody sensitive to the privacy of his own data, but still willing to store them in the cloud, might be tempted to install the feature-rich OwnCloud application on a dedicated server. Even more interestingly, the feature list of the latest version mentions the following:

Do you want to make sure that your files remain secure on the server? With the Encryption Application enabled, all files stored on the ownCloud server are encrypted to your password so not even the admin can look inside your files. Add to this an SSL connection, and your files are secure while in motion and at rest.

I did not resist to take a closer look at these claims...

The file encryption capabilities are implemented as the `OC_Crypt` class. Here is a quick summary of my findings:

- The key is generated using four calls to the `mt_rand()` PHP routine, which implements the *Mersenne Twister* pseudo-random generator and is unfortunately **not** of cryptographic quality:

```
1 public static function createkey($username,$password) {
2 // generate a random key
3 $key=mt_rand(10000,99999).mt_rand(10000,99999).mt_rand(10000,99999).mt_
4
5 // encrypt the key with the passcode of the user
6 $senkey=OC_Crypt::encrypt($key,$password);
7
8 // Write the file
9 $proxyEnabled=OC_FileProxy::$enabled;
10 OC_FileProxy::$enabled=false;
11 $view=new OC_FileSystemView('/', $username);
12 $view->file_put_contents('/encryption.key',$senkey);
13 OC_FileProxy::$enabled=$proxyEnabled;
14 }
```

- In retrospective: Consider publishing advisories first after you consider your project secure enough.

- Reviews will come anyways.
- Best to be pro-active and have stuff fixed before.
- Bug bounty a good addition to external reviews.
  - ... consider starting with higher rewards though.

**Do not trust reviews without checking them in detail.**

# Don't fix single bugs

... fix the categories of bugs and do root cause analysis.



# Thanks!

[github.com/owncloud](https://github.com/owncloud)

[hackerone.com/owncloud](https://hackerone.com/owncloud)

