WoSign Incidents Report

(September 4th 2016)

WoSign got email notice from Mozilla for 3 incidents about WoSign at August 24th 2016, and WoSign responded to the inquiry emails from Mozilla-Dev-Security-Policy mail list, this is the formal report about the details of the incidents, we'd like the make it transparency to everybody to know what happened and what we learn from these incidents.

1. Incident 0

1.1. Message from Mozilla

(The italic section is the original message from Mozilla)

On or around April 23rd, 2015, WoSign's certificate issuance system for their free certificates allowed the applicant to choose any port for validation. Once validation had been completed, WoSign would issue certificates for that domain. A researcher was able to obtain a certificate for a university by opening a high-numbered port (>50,000) and getting WoSign to use that port for validation of control.

This problem was reported to Google, and thence to WoSign and resolved.
Mozilla only became aware of it recently.

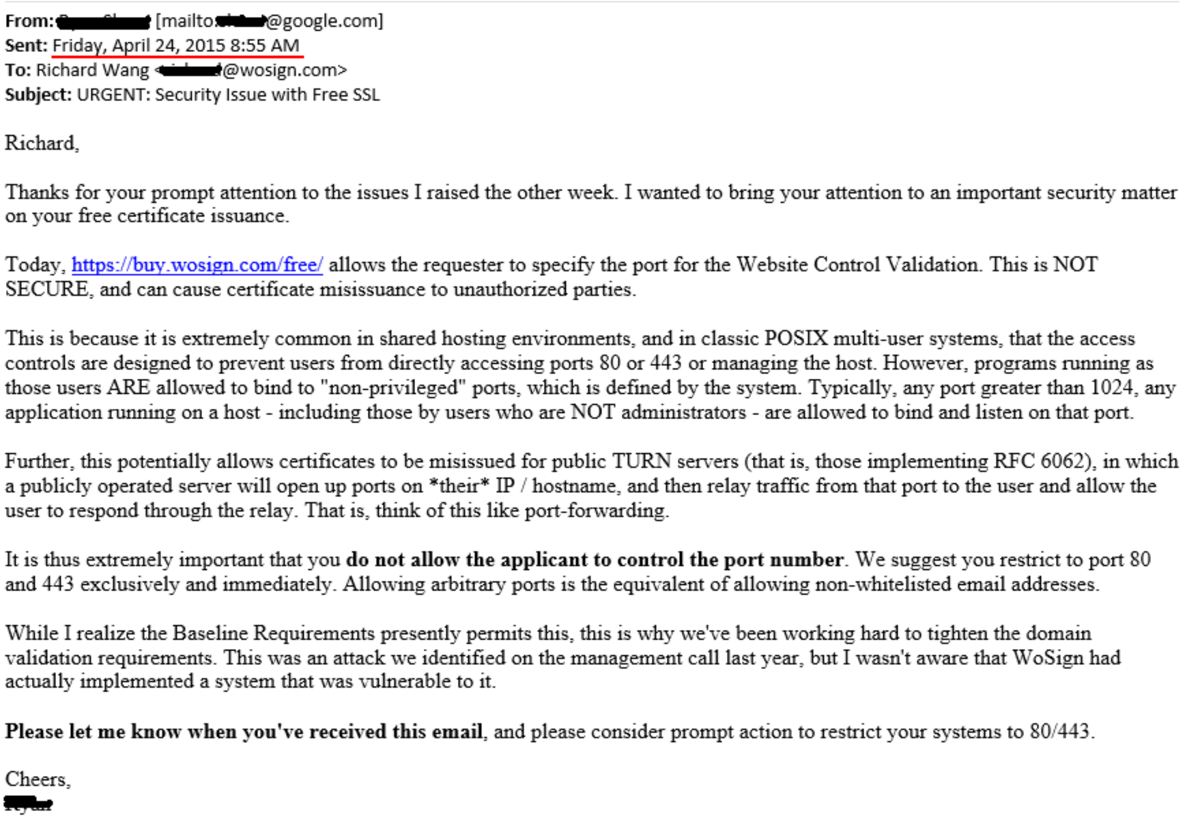
** Before the recent passage of Ballot 169 in the CAB Forum, which limits the ports and paths which can be used, the Baseline Requirements said that one acceptable method of domain validation was "Having the Applicant demonstrate practical control over the FQDN by making an agreed‐upon change to information found on an online Web page identified by a uniform resource identifier containing the FQDN". This method therefore did not violate the letter of the BRs. However, Mozilla considers the basic security knowledge that ports over 1024 are unprivileged should have led all CAs not to accept validations of domain control on such ports, even when not documented in the BRs.*

** The misissuance incident was not reported to Mozilla by WoSign as it should have been (see above).*

** This misissuance incident did not turn up on WoSign's subsequent BR audit.*

1.2. Incident Response

WoSign got report from Google at **<u>8:55</u> AM April 24th 2015** (Beijing time, UTC+8:00, same for all time in this report), see Figure 1:



From: [redacted] [mailto:[redacted]@google.com]
Sent: Friday, April 24, 2015 8:55 AM
To: Richard Wang <[redacted]@wosign.com>
Subject: URGENT: Security Issue with Free SSL

Richard,

Thanks for your prompt attention to the issues I raised the other week. I wanted to bring your attention to an important security matter on your free certificate issuance.

Today, https://buy.wosign.com/free/ allows the requester to specify the port for the Website Control Validation. This is NOT SECURE, and can cause certificate misissuance to unauthorized parties.

This is because it is extremely common in shared hosting environments, and in classic POSIX multi-user systems, that the access controls are designed to prevent users from directly accessing ports 80 or 443 or managing the host. However, programs running as those users ARE allowed to bind to "non-privileged" ports, which is defined by the system. Typically, any port greater than 1024, any application running on a host - including those by users who are NOT administrators - are allowed to bind and listen on that port.

Further, this potentially allows certificates to be misissued for public TURN servers (that is, those implementing RFC 6062), in which a publicly operated server will open up ports on *their* IP / hostname, and then relay traffic from that port to the user and allow the user to respond through the relay. That is, think of this like port-forwarding.

It is thus extremely important that you **do not allow the applicant to control the port number**. We suggest you restrict to port 80 and 443 exclusively and immediately. Allowing arbitrary ports is the equivalent of allowing non-whitelisted email addresses.

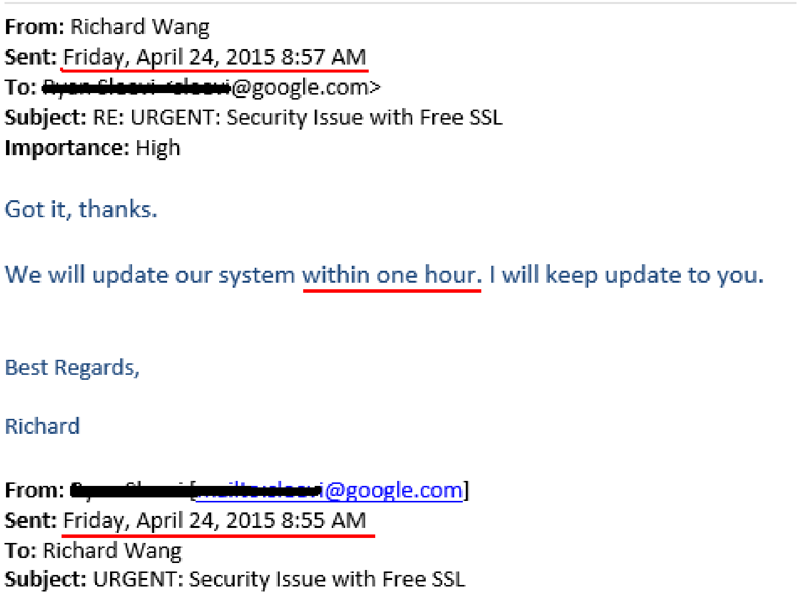
While I realize the Baseline Requirements presently permits this, this is why we've been working hard to tighten the domain validation requirements. This was an attack we identified on the management call last year, but I wasn't aware that WoSign had actually implemented a system that was vulnerable to it.

Please let me know when you've received this email, and please consider prompt action to restrict your systems to 80/443.

Cheers,
[redacted]

Figure 1

Richard Wang, the CEO of WoSign replied Google email within **2 minutes** after receiving the report email, and promised to fix this bug within **1 hour**, see Figure 2:



From: Richard Wang
Sent: Friday, April 24, 2015 8:57 AM
To: [redacted]@google.com>
Subject: RE: URGENT: Security Issue with Free SSL
Importance: High

Got it, thanks.

We will update our system within one hour. I will keep update to you.

Best Regards,

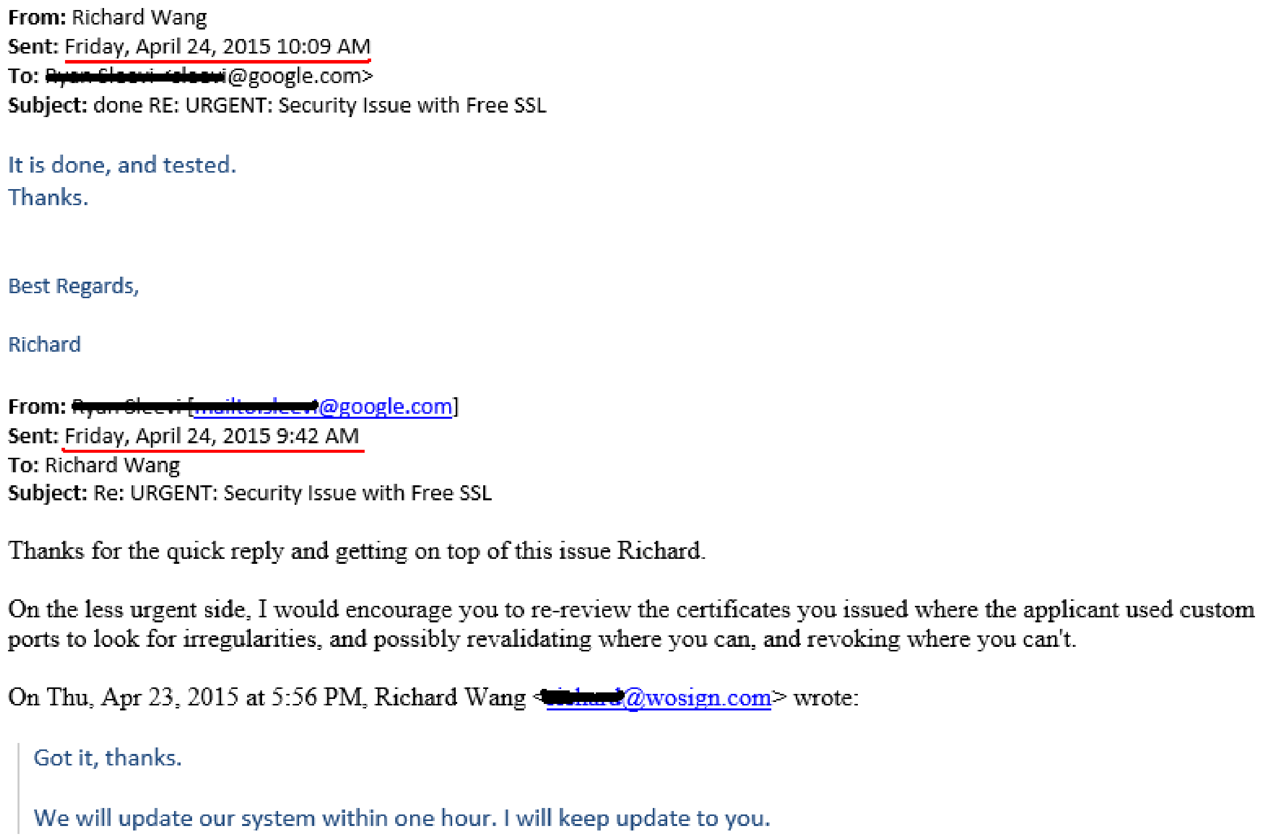
Richard

From: [redacted] [[redacted]@google.com]
Sent: Friday, April 24, 2015 8:55 AM
To: Richard Wang
Subject: URGENT: Security Issue with Free SSL

Figure 2

Richard sent email to Google at 10:09AM after fixed the bug. The whole process including notify the

RD team, modify the code, test in testing system, upload to website, and test in production system, send email to Google, only took one hour and 10 minutes, 10 minutes late as Richard promised to Google, see Figure 3:



From: Richard Wang
Sent: Friday, April 24, 2015 10:09 AM
To: [redacted]i@google.com>
Subject: done RE: URGENT: Security Issue with Free SSL

It is done, and tested.
Thanks.

Best Regards,

Richard

From: [redacted]@google.com]
Sent: Friday, April 24, 2015 9:42 AM
To: Richard Wang
Subject: Re: URGENT: Security Issue with Free SSL

Thanks for the quick reply and getting on top of this issue Richard.

On the less urgent side, I would encourage you to re-review the certificates you issued where the applicant used custom ports to look for irregularities, and possibly revalidating where you can, and revoking where you can't.

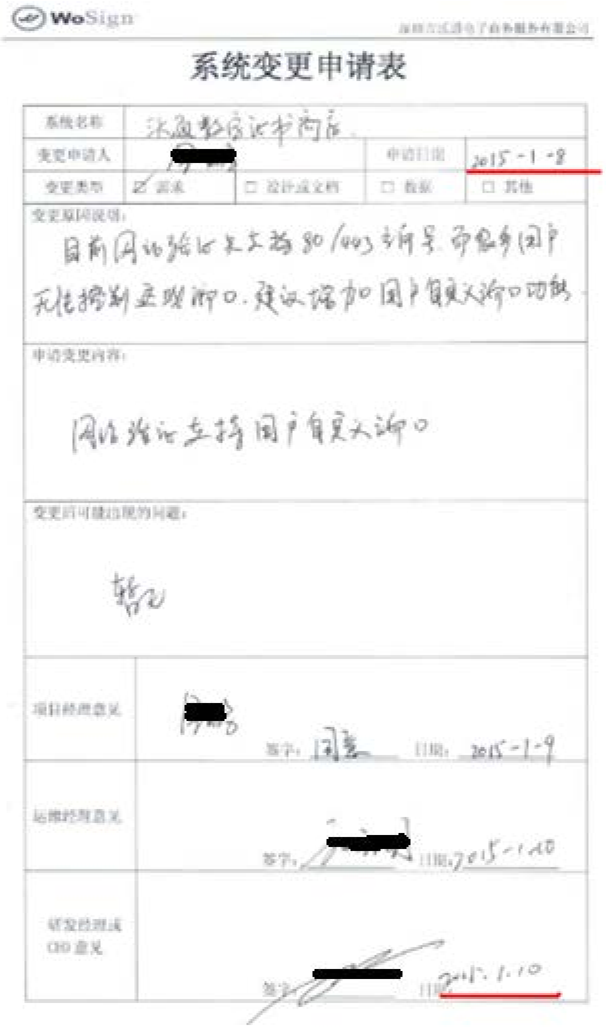
On Thu, Apr 23, 2015 at 5:56 PM, Richard Wang <[redacted]@wosign.com> wrote:

> Got it, thanks.
>
> We will update our system within one hour. I will keep update to you.

Figure 3

1.3. Cause of the Incident

WoSign checked the system change logs, this change was approved on Jan. 10th 2015 (see Figure 4). The reason was some customer can't use the 80 or 443 port to do the domain validation and asking for any port validation. The Figure 5 shows we changed our system to fix the problem that Google reported on April 24th 2015 and closed all ports except 80 and 443. So the high port validation allowed period is from Jan. 10th, 2015 to April 24th, 2015.



WoSign 深圳市沃通电子商务服务有限公司

系统变更申请表

系统名称	沃通数字证书商店		
变更申请人	[redacted]	申请日期	2015-1-8
变更类型	☑ 需求	□ 设计或文档	□ 数据 □ 其他

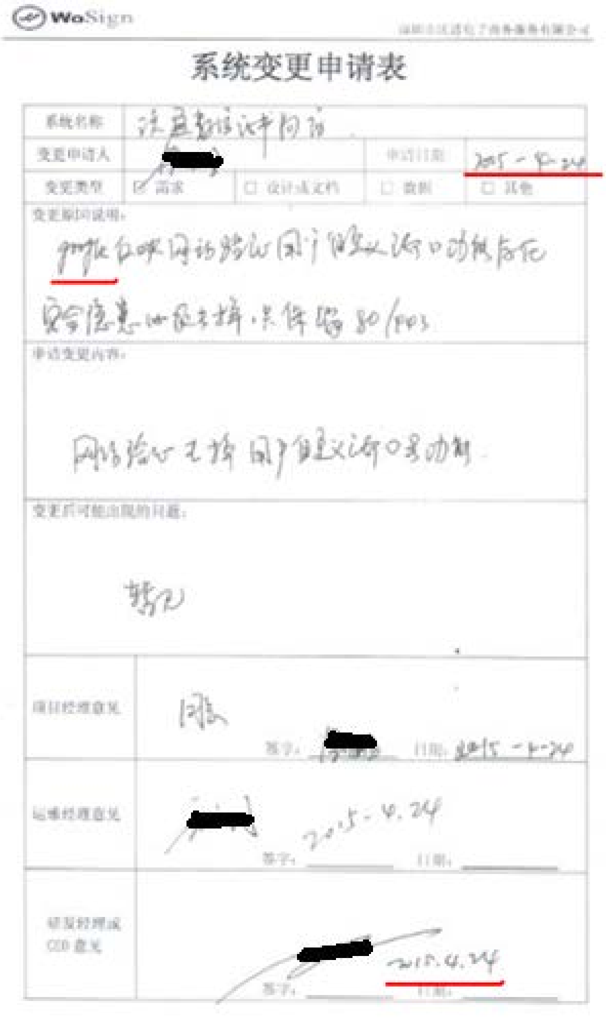
变更原因说明：
目前网站验证只支持80/443端口，部分客户无法控制这些端口。建议增加用户自定义端口功能

申请变更内容：
网站验证支持用户自定义端口

变更后可能出现的问题：
暂无

项目经理意见	[redacted] 签字：同意 日期：2015-1-9
运维经理意见	签字：[redacted] 日期：2015-1-10
研发经理或CTO意见	签字：[redacted] 日期：2015.1.10

Figure 4



WoSign 深圳市沃通电子商务服务有限公司

系统变更申请表

系统名称	沃通数字证书商店		
变更申请人	[redacted]	申请日期	2015-4-24
变更类型	☑ 需求	□ 设计或文档	□ 数据 □ 其他

变更原因说明：
google反映网站验证用户自定义端口功能存在安全隐患，需取消，只保留80/443

申请变更内容：
网站验证取消用户自定义端口功能

变更后可能出现的问题：
暂无

项目经理意见	同意 签字：[redacted] 日期：2015-4-24
运维经理意见	[redacted] 2015-4.24 签字： 日期：
研发经理或CTO意见	[redacted] 2015.4.24 签字： 日期：

Figure 5

1.4. Impact Analytics

We searched our certificates orders from January 10th 2015 to April 24th 2015, there were 72 certificates issued using higher numbered ports website control validation, those certificates were validated by website control validation method that using other port instead of 80 and 443, we investigated each certificates to think it is no necessary to revoke these certificates. We posted all those certificates to WoSign CT log server at Aug. 26th 2016 and Google CT log server at Sept. 03rd 2016.

Here is the crt.sh link for all 72 certificates:
https://crt.sh/?id=29805572
https://crt.sh/?id=7022909
https://crt.sh/?id=7564839
https://crt.sh/?id=29805573
https://crt.sh/?id=29805574
https://crt.sh/?id=29805575
https://crt.sh/?id=29805576
https://crt.sh/?id=29805577

https://crt.sh/?id=6969460
https://crt.sh/?id=29805578
https://crt.sh/?id=29805579
https://crt.sh/?id=29805580
https://crt.sh/?id=29805581
https://crt.sh/?id=29805582
https://crt.sh/?id=29805584
https://crt.sh/?id=29805585
https://crt.sh/?id=29805586
https://crt.sh/?id=9911443
https://crt.sh/?id=29805587
https://crt.sh/?id=7122803
https://crt.sh/?id=29805588
https://crt.sh/?id=29805589
https://crt.sh/?id=9985267
https://crt.sh/?id=29805590
https://crt.sh/?id=29805591
https://crt.sh/?id=29805592
https://crt.sh/?id=29805593
https://crt.sh/?id=29805594
https://crt.sh/?id=7224978
https://crt.sh/?id=10917791
https://crt.sh/?id=29805595
https://crt.sh/?id=29805596
https://crt.sh/?id=29805597
https://crt.sh/?id=6788465
https://crt.sh/?id=7224923
https://crt.sh/?id=9169568
https://crt.sh/?id=6836953
https://crt.sh/?id=29805598
https://crt.sh/?id=8172756
https://crt.sh/?id=29805599
https://crt.sh/?id=29805600
https://crt.sh/?id=7021184
https://crt.sh/?id=29805601
https://crt.sh/?id=29805602
https://crt.sh/?id=29805603
https://crt.sh/?id=29805604
https://crt.sh/?id=6927114
https://crt.sh/?id=6777468
https://crt.sh/?id=9793847
https://crt.sh/?id=29805605
https://crt.sh/?id=29805606
https://crt.sh/?id=29805607
https://crt.sh/?id=29805608
https://crt.sh/?id=9932344

https://crt.sh/?id=29805609
https://crt.sh/?id=29805610
https://crt.sh/?id=6880740
https://crt.sh/?id=29805611
https://crt.sh/?id=29805612
https://crt.sh/?id=7015627
https://crt.sh/?id=10008992
https://crt.sh/?id=29805613
https://crt.sh/?id=29805614
https://crt.sh/?id=29805615
https://crt.sh/?id=29805616
https://crt.sh/?id=7046181
https://crt.sh/?id=29805617
https://crt.sh/?id=29805618
https://crt.sh/?id=29805619
https://crt.sh/?id=7121749
https://crt.sh/?id=29805620
https://crt.sh/?id=6999366

2. Incident 1

2.1. Message from Mozilla

In June 2015, an applicant found a problem with WoSign's free certificate service, which allowed them to get a certificate for the base domain if they were able to prove control of a subdomain.

The reporter proved the problem in two ways. They accidentally discovered it when trying to get a certificate for med.ucf.edu and mistakenly also applied for www.ucf.edu, which was approved. They then confirmed the problem by using their control of theiraccount.github.com/theiraccount.github.io to get a cert for github.com, github.io, and www.github.io.

They reported this to WoSign, giving only the Github certificate as an example. That cert was revoked and the vulnerability was fixed. However recently, they got in touch with Google to note that the ucf.edu cert still had not been revoked almost a year later.

** The lack of revocation of the ucf.edu certificate (still unrevoked at time of writing, although it may have been by time of posting) strongly suggests that WoSign either did not or could not search their issuance databases for other occurrences of the same problem. Mozilla considers such a search a basic part of the response to disclosure of a vulnerability which causes misissuance, and expects CAs to keep records detailed enough to make it possible.*

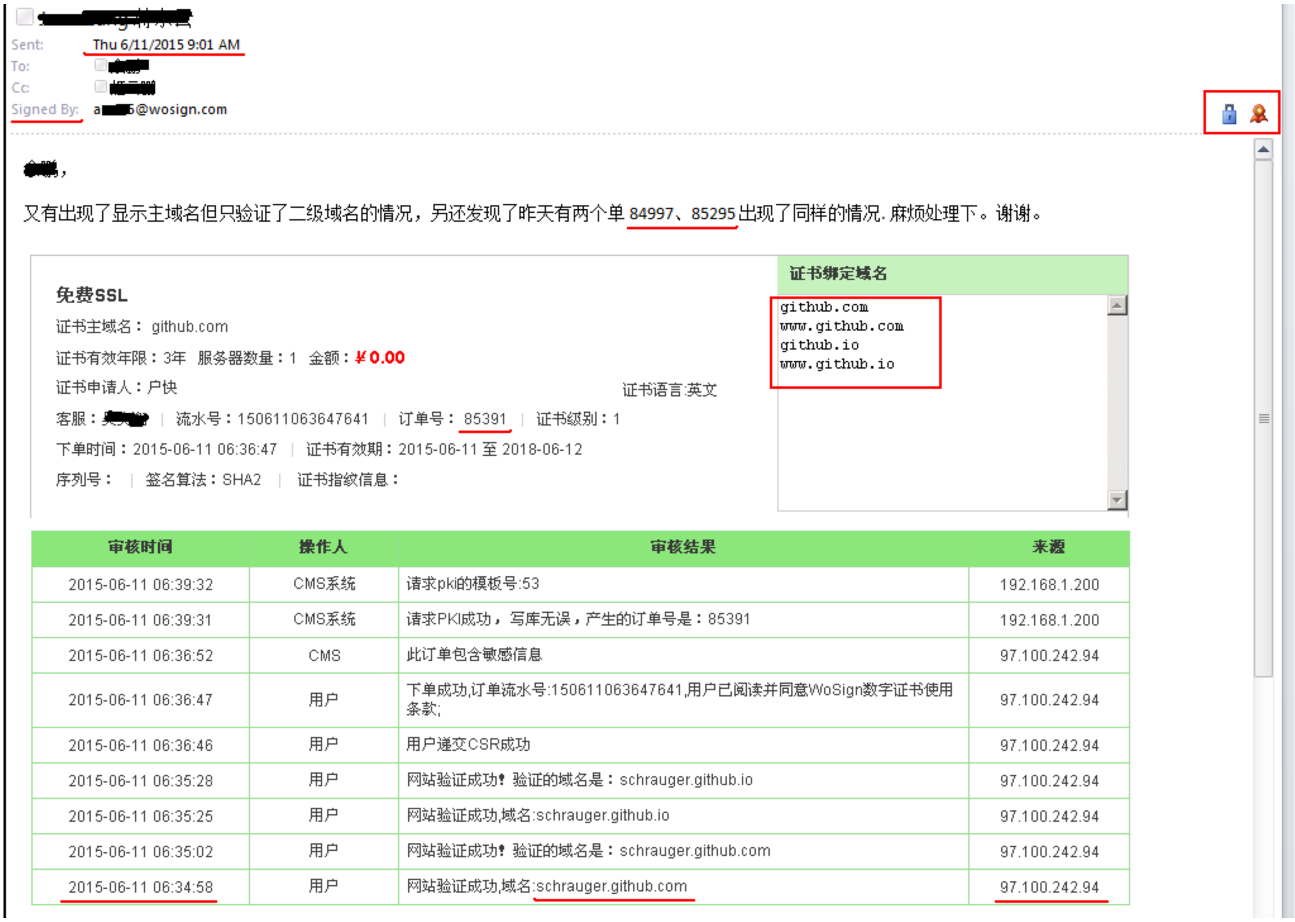
** This misissuance incident was not reported to Mozilla by WoSign as it should have been (see above).*

** This misissuance incident did not turn up on WoSign's subsequent BR audit.*

There are 2 vulnerabilities/bugs triggered this incident.

2.2. Github.com domain case

Let’s explain the Github domain case first since there are inaccurate information in some articles. The subscriber (IP: 97.100.242.94, account email: github-wosign.com@orders.schrauger.com) passed the website control validation for subdomain: “schrauger.github.io” at **June 11, 2015 06:34:58**, this order was passed to the human review process because the domain “github” was tagged in system that the certificates need to be issued manually, this order was reviewed by validation team, the validation team found that the domain related with another two orders (84997, 85295) that the certificates already been issued. The following email screenshot (see Figure 6) shows that the finding time was **June 11 2015 09:01 AM** that the validation team start their daily work. Please notice that the email encryption and digital signature icon in the left from Outlook can be a trusted proof document for the event time.



[redacted]

Sent: Thu 6/11/2015 9:01 AM

To: [redacted]

Cc: [redacted]

Signed By: a[redacted]6@wosign.com

[redacted]，

又有出现了显示主域名但只验证了二级域名的情况，另还发现了昨天有两个单 84997、85295 出现了同样的情况. 麻烦处理下。谢谢。

免费SSL

证书主域名： github.com

证书有效年限：3年　服务器数量：1　金额：¥0.00

证书申请人：户快　　　　证书语言:英文

客服：[redacted] | 流水号：150611063647641 | 订单号： 85391 | 证书级别：1

下单时间：2015-06-11 06:36:47 | 证书有效期：2015-06-11 至 2018-06-12

序列号： | 签名算法：SHA2 | 证书指纹信息：

证书绑定域名

github.com
www.github.com
github.io
www.github.io

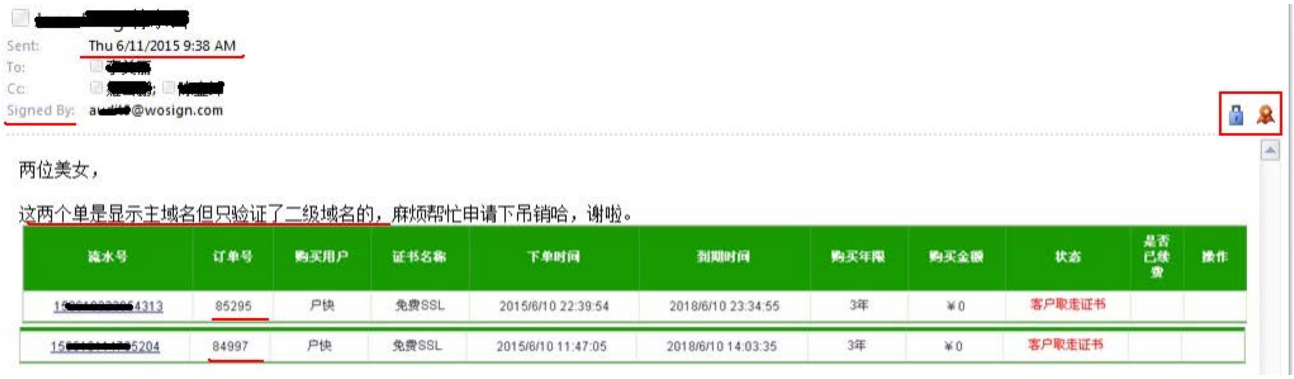
审核时间	操作人	审核结果	来源
2015-06-11 06:39:32	CMS系统	请求pki的模板号:53	192.168.1.200
2015-06-11 06:39:31	CMS系统	请求PKI成功，写库无误，产生的订单号是：85391	192.168.1.200
2015-06-11 06:36:52	CMS	此订单包含敏感信息	97.100.242.94
2015-06-11 06:36:47	用户	下单成功,订单流水号:150611063647641,用户已阅读并同意WoSign数字证书使用条款;	97.100.242.94
2015-06-11 06:36:46	用户	用户递交CSR成功	97.100.242.94
2015-06-11 06:35:28	用户	网站验证成功! 验证的域名是：schrauger.github.io	97.100.242.94
2015-06-11 06:35:25	用户	网站验证成功,域名:schrauger.github.io	97.100.242.94
2015-06-11 06:35:02	用户	网站验证成功! 验证的域名是：schrauger.github.com	97.100.242.94
2015-06-11 06:34:58	用户	网站验证成功,域名:schrauger.github.com	97.100.242.94

Figure 6

So the validation team rejected this order, and sent email to the revocation team to revoke the two mis-issued certificates for github, the email time is **June 11 2105 09:38 AM**, see Figure 7. It said:

“Hi two beautiful girls, //the revocation process need two employee for double checking
The following two order is mis-issued that only validated the subdomain, the top domain don’t be validated, so please revoke the two certificates, thanks.”

This email pasted the two order's detail screenshot with order number: 84997, 85295, see Figure 7:



[redacted]

Sent: Thu 6/11/2015 9:38 AM
To: [redacted]
Cc: [redacted]; [redacted]
Signed By: a[redacted]@wosign.com

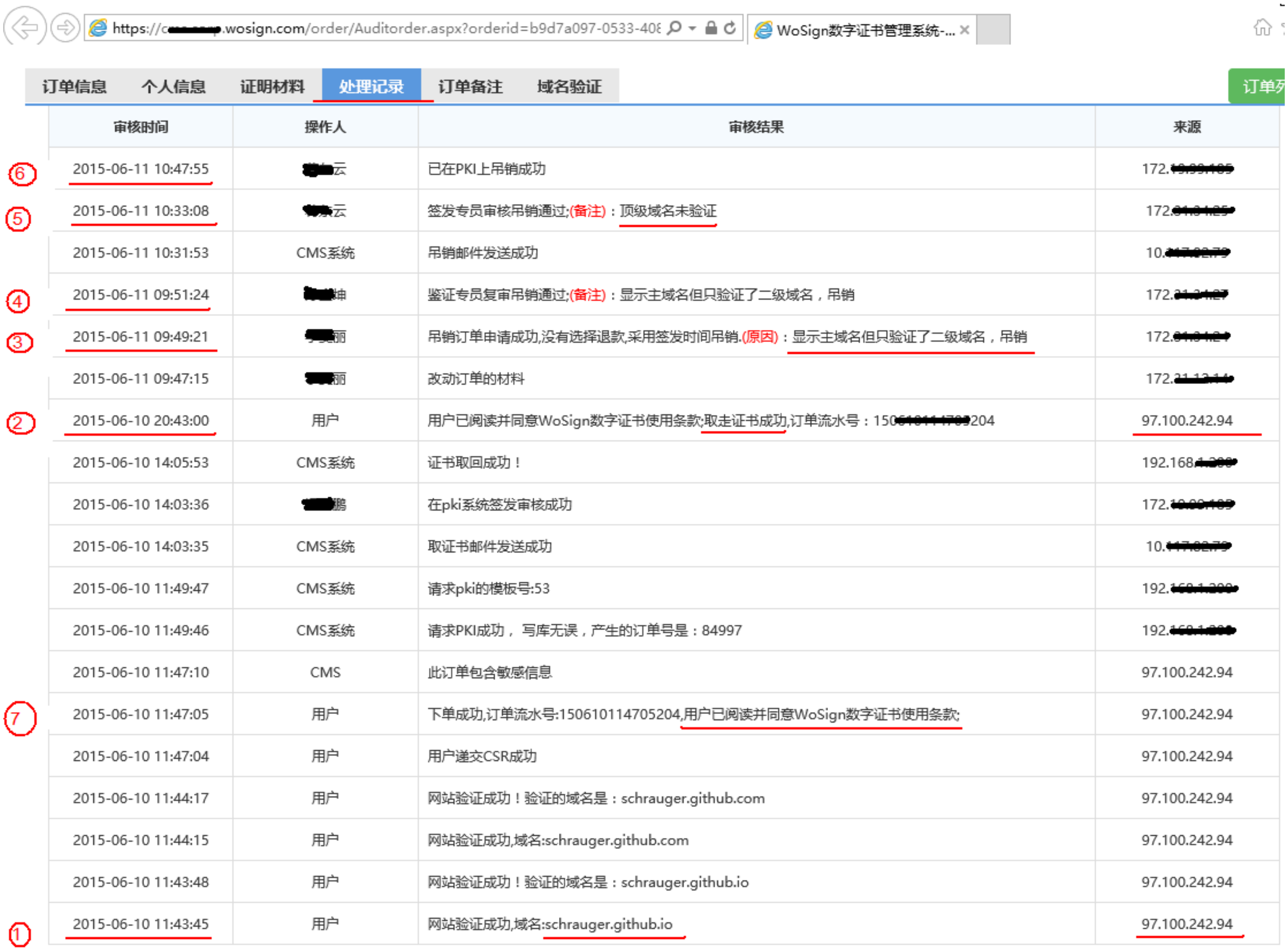
两位美女，

这两个单是显示主域名但只验证了二级域名的，麻烦帮忙申请下吊销哈，谢啦。

流水号	订单号	购买用户	证书名称	下单时间	到期时间	购买年限	购买金额	状态	是否已续费	操作
1[redacted]4313	85295	户快	免费SSL	2015/6/10 22:39:54	2018/6/10 23:34:55	3年	¥0	客户取走证书		
15[redacted]5204	84997	户快	免费SSL	2015/6/10 11:47:05	2018/6/10 14:03:35	3年	¥0	客户取走证书		

Figure 7

For the revoked certificate (order No. 84997, https://crt.sh/?id=29647048), here is the order processing log, please notice the log record time is consistent with the above email signature time to proof the authenticity, see Figure 8. (the log time format is YYYY-MM-DD HH:MM:SS)


https://c[redacted].wosign.com/order/Auditorder.aspx?orderid=b9d7a097-0533-408
WoSign数字证书管理系统-...
订单信息
个人信息
证明材料
处理记录
订单备注
域名验证
订单列

	审核时间	操作人	审核结果	来源
⑥	2015-06-11 10:47:55	[redacted]云	已在PKI上吊销成功	172.[redacted]
⑤	2015-06-11 10:33:08	[redacted]云	签发专员审核吊销通过;(备注)：顶级域名未验证	172.[redacted]
	2015-06-11 10:31:53	CMS系统	吊销邮件发送成功	10.[redacted]
④	2015-06-11 09:51:24	[redacted]坤	鉴证专员复审吊销通过;(备注)：显示主域名但只验证了二级域名，吊销	172.[redacted]
③	2015-06-11 09:49:21	[redacted]丽	吊销订单申请成功,没有选择退款,采用签发时间吊销.(原因)：显示主域名但只验证了二级域名，吊销	172.[redacted]
	2015-06-11 09:47:15	[redacted]丽	改动订单的材料	172.[redacted]
②	2015-06-10 20:43:00	用户	用户已阅读并同意WoSign数字证书使用条款;取走证书成功,订单流水号：150[redacted]204	97.100.242.94
	2015-06-10 14:05:53	CMS系统	证书取回成功！	192.168[redacted]
	2015-06-10 14:03:36	[redacted]鹏	在pki系统签发审核成功	172.[redacted]
	2015-06-10 14:03:35	CMS系统	取证书邮件发送成功	10.[redacted]
	2015-06-10 11:49:47	CMS系统	请求pki的模板号:53	192.[redacted]
	2015-06-10 11:49:46	CMS系统	请求PKI成功， 写库无误，产生的订单号是：84997	192.[redacted]
	2015-06-10 11:47:10	CMS	此订单包含敏感信息	97.100.242.94
⑦	2015-06-10 11:47:05	用户	下单成功,订单流水号:150610114705204,用户已阅读并同意WoSign数字证书使用条款;	97.100.242.94
	2015-06-10 11:47:04	用户	用户递交CSR成功	97.100.242.94
	2015-06-10 11:44:17	用户	网站验证成功！验证的域名是：schrauger.github.com	97.100.242.94
	2015-06-10 11:44:15	用户	网站验证成功,域名:schrauger.github.com	97.100.242.94
	2015-06-10 11:43:48	用户	网站验证成功！验证的域名是：schrauger.github.io	97.100.242.94
①	2015-06-10 11:43:45	用户	网站验证成功,域名:schrauger.github.io	97.100.242.94

Figure 8

(1) **2015-06-10 11:43:45**: subdomain: schrauger.github.io passed the website control validation, the subscriber IP is 97.100.242.94, same as the rejected order;
(2) **2015-06-10 20:43:00**: subscriber retrieved the certificate, IP: 97.100.242.94
(3) **2015-06-11 09:49:21**: "Validation Team A" initialed the revocation request, she got email at **09:38**, this means she took 11 minutes to review this order, the revocation reason is "this order validated the subdomain only, but the certificate included the top domain, must revoke this certificate";
(4) **2015-06-11 09:51:24**: 2 minutes later, "Validation Team B" reviewed the revocation request, and approved this request. The next log record says "system sent the revocation email to subscriber";
(5) **2015-06-11 10:33:08**: The PKI Admin (another person) approved this revocation request in PKI (42 minutes later), the reason is "top domain not validated";
(6) **2015-06-11 10:47:55**: PKI system return the revocation success.

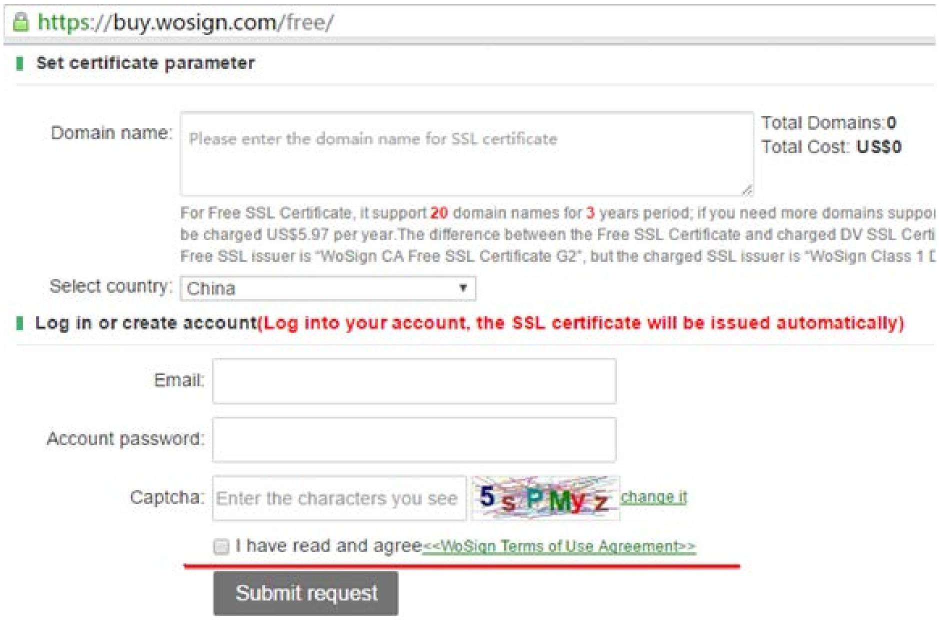
From the log, we can see this mis-issued certificate was founded on the next day morning, the first work for validation tem is to review the certificates issued last day, then it took **1 hour and 48 minutes** to revoke this certificate.

Please notice **log (7)**, the time is **2015-06-10 11:47:05**, it says "the subscriber read and agreed the term of use", please refer to WoSign term of use agreement (complied with BR 9.6.3):

https://www.wosign.com/policy/Terms_of_Use_Agreement.pdf

"5. Reporting and Revocation: An obligation and warranty to promptly cease using a Certificate and its associated Private Key, and promptly request WoSign to revoke the Certificate, in the event that: (a) any information in the Certificate is, or becomes, incorrect or inaccurate, or (b) there is any actual or suspected misuse or compromise of the Subscriber's Private Key associated with the Public Key included in the Certificate".

This is the screenshot of ordering a certificate that subscriber must click the agree button to read and agree the TOU agreement:



https://buy.wosign.com/free/

Set certificate parameter

Domain name: Please enter the domain name for SSL certificate

Total Domains:0
Total Cost: US$0

For Free SSL Certificate, it support 20 domain names for 3 years period; if you need more domains suppo
be charged US$5.97 per year.The difference between the Free SSL Certificate and charged DV SSL Certi
Free SSL issuer is "WoSign CA Free SSL Certificate G2", but the charged SSL issuer is "WoSign Class 1 [

Select country: China ▾

Log in or create account(Log into your account, the SSL certificate will be issued automatically)

Email:

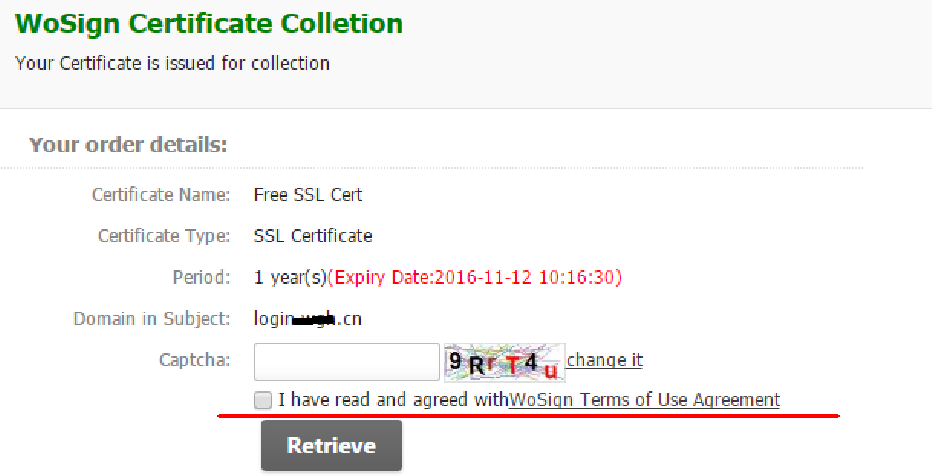
Account password:

Captcha: Enter the characters you see

□ I have read and agree<<WoSign Terms of Use Agreement>>

Figure 9

And this is the screenshot of retrieving the issued certificate, the subscriber must click the agree button to read and agree the TOU agreement again:



WoSign Certificate Colletion

Your Certificate is issued for collection

Your order details:

Certificate Name:	Free SSL Cert
Certificate Type:	SSL Certificate
Period:	1 year(s)(Expiry Date:2016-11-12 10:16:30)
Domain in Subject:	login[redacted].cn
Captcha:	9RrT4u change it

□ I have read and agreed withWoSign Terms of Use Agreement

Retrieve

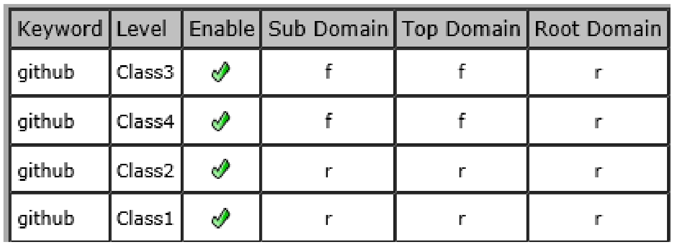
Figure 10

This subscriber agreed the TOU to submit the order and get the certificate, but he didn't report to WoSign to revoke this certificate (without reported at time of Mozilla writing). But he used this case as evidence to write article in his website to public.

2.2.1 Cause of the incident

This mis-issued certificate was a system vulnerability that when the subscriber finished the domain validation, they can add any domain before submitting this order to system. WoSign don't know this vulnerability even when we found the mis-issued certificate for github.com, the employee treated it as an unusual case that did not reported it as a bug, the vulnerability got fixed on the August 10, 2015 system upgrade, this upgrade changed the order procedure that subscriber submit the all domains first to database, then validate it one by one, the vulnerability was fixed.

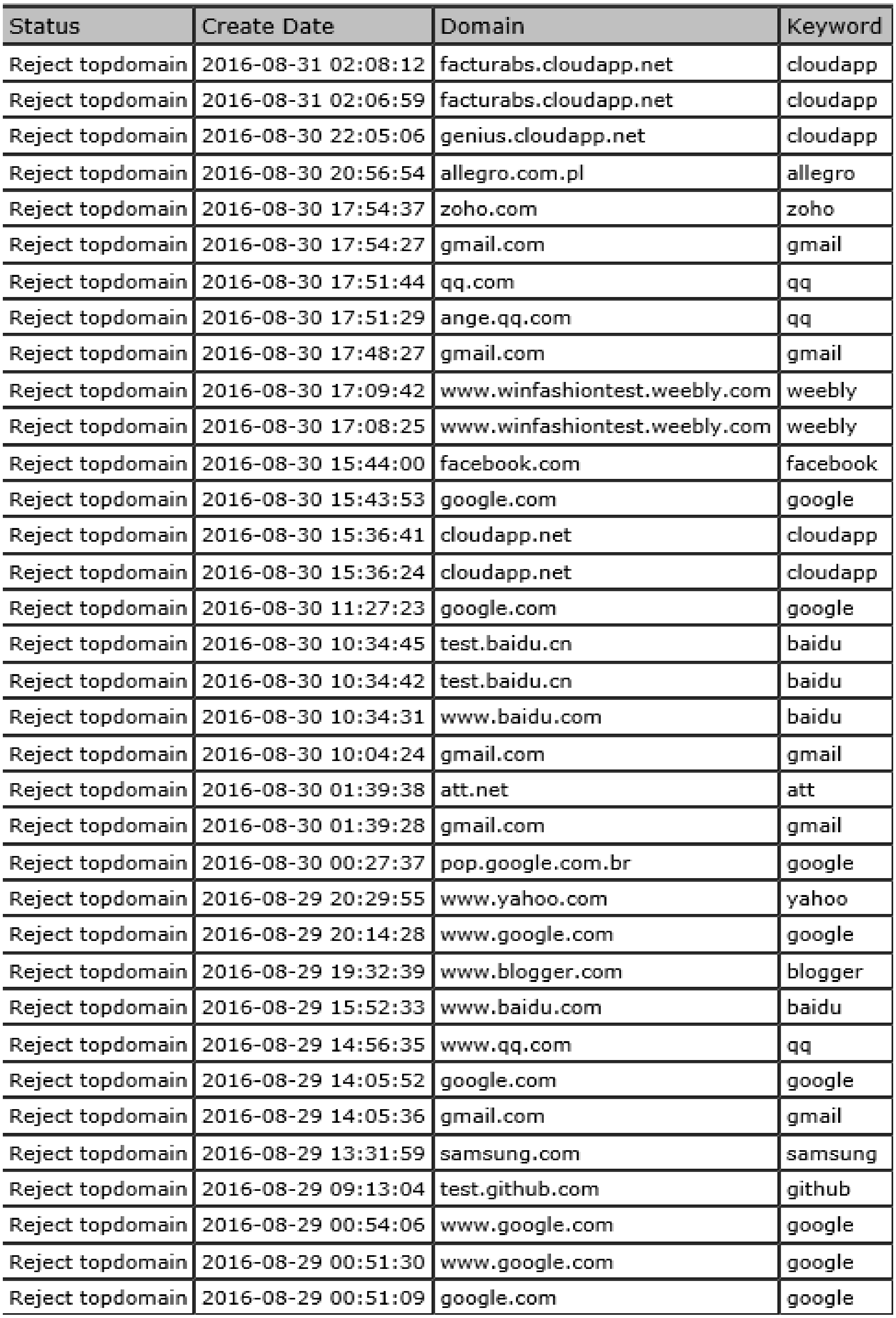
We searched our database after we got the notification from Mozilla, we found there are 12 certificates mis-issued with this vulnerability including the certificate issued to the domain "med.ucf.edu", all are not the normal order that use a special professional method to get this type of certificate that the subscribers must report to WoSign to revoke those certificates according to TOU. The reason that we found the github issue but did not found others is we have a protected domain list that github is in the list, other mis-issued certificate is not recognized as a famous brand that not in the list and was issued automatically.
The following screenshot is the current keyword setting for github, "f"=flag; "r"=reject, we changed the class 1 certificate from "f" to "r" after we found out the mis-issued certificate case for github.



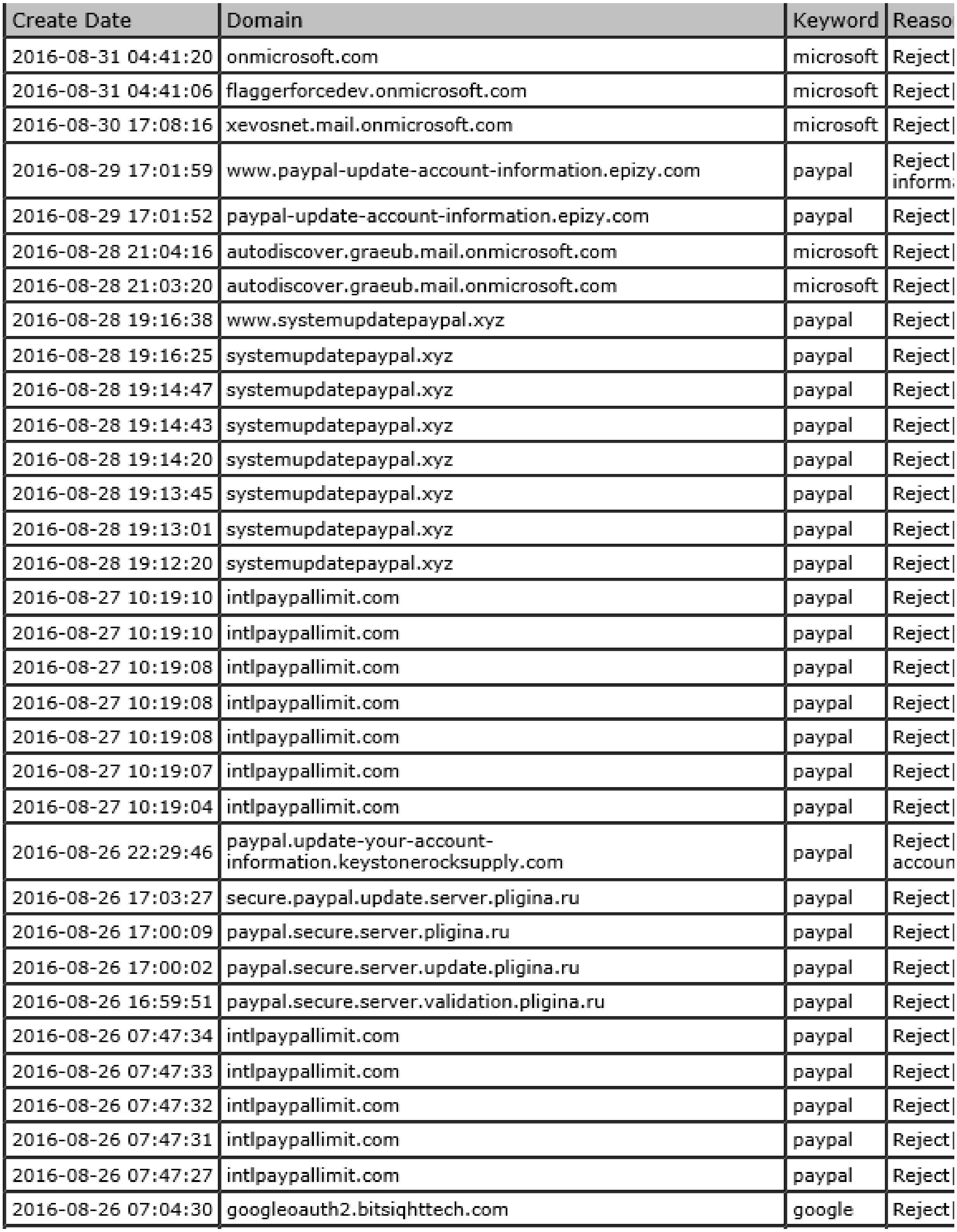
Keyword	Level	Enable	Sub Domain	Top Domain	Root Domain
github	Class3	✓	f	f	r
github	Class4	✓	f	f	r
github	Class2	✓	r	r	r
github	Class1	✓	r	r	r

Figure 11

System blocked many illegal request every day, the following screen shot is the reject order log:



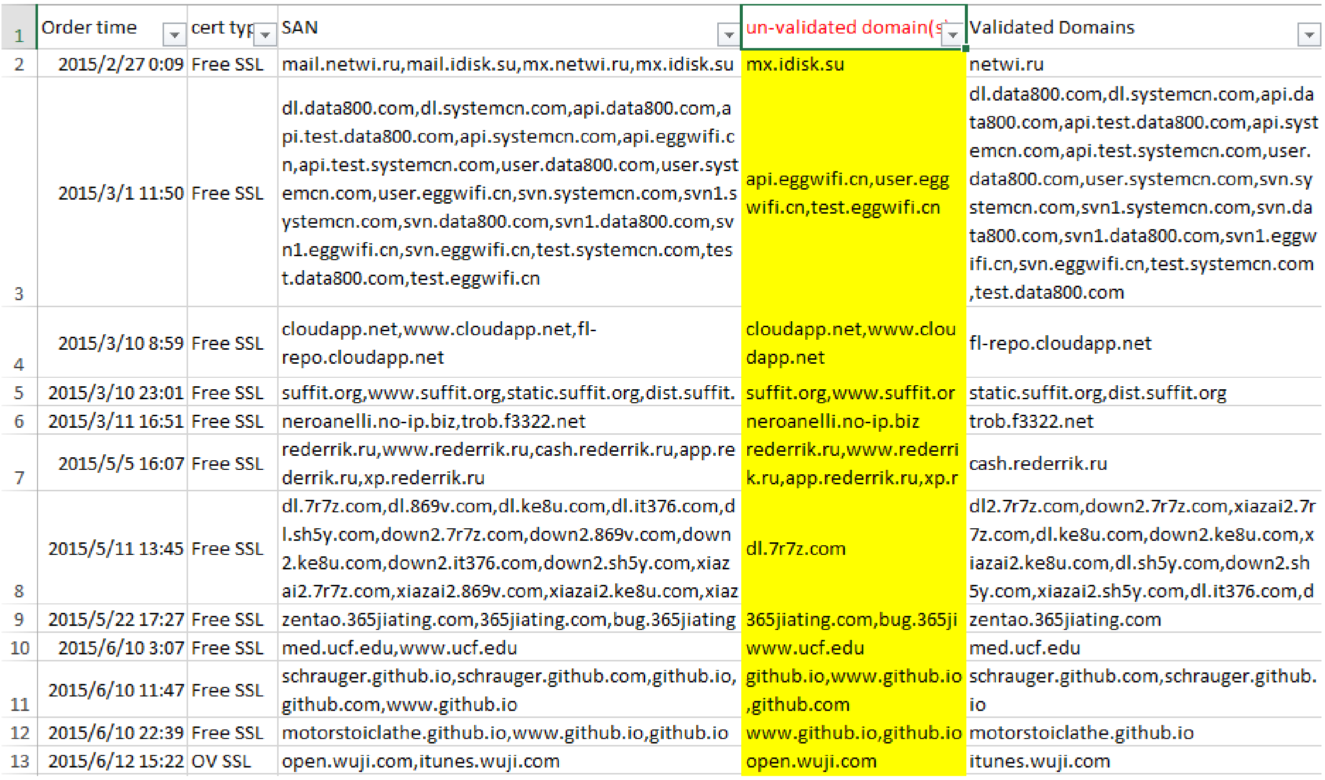
Status	Create Date	Domain	Keyword
Reject topdomain	2016-08-31 02:08:12	facturabs.cloudapp.net	cloudapp
Reject topdomain	2016-08-31 02:06:59	facturabs.cloudapp.net	cloudapp
Reject topdomain	2016-08-30 22:05:06	genius.cloudapp.net	cloudapp
Reject topdomain	2016-08-30 20:56:54	allegro.com.pl	allegro
Reject topdomain	2016-08-30 17:54:37	zoho.com	zoho
Reject topdomain	2016-08-30 17:54:27	gmail.com	gmail
Reject topdomain	2016-08-30 17:51:44	qq.com	qq
Reject topdomain	2016-08-30 17:51:29	ange.qq.com	qq
Reject topdomain	2016-08-30 17:48:27	gmail.com	gmail
Reject topdomain	2016-08-30 17:09:42	www.winfashiontest.weebly.com	weebly
Reject topdomain	2016-08-30 17:08:25	www.winfashiontest.weebly.com	weebly
Reject topdomain	2016-08-30 15:44:00	facebook.com	facebook
Reject topdomain	2016-08-30 15:43:53	google.com	google
Reject topdomain	2016-08-30 15:36:41	cloudapp.net	cloudapp
Reject topdomain	2016-08-30 15:36:24	cloudapp.net	cloudapp
Reject topdomain	2016-08-30 11:27:23	google.com	google
Reject topdomain	2016-08-30 10:34:45	test.baidu.cn	baidu
Reject topdomain	2016-08-30 10:34:42	test.baidu.cn	baidu
Reject topdomain	2016-08-30 10:34:31	www.baidu.com	baidu
Reject topdomain	2016-08-30 10:04:24	gmail.com	gmail
Reject topdomain	2016-08-30 01:39:38	att.net	att
Reject topdomain	2016-08-30 01:39:28	gmail.com	gmail
Reject topdomain	2016-08-30 00:27:37	pop.google.com.br	google
Reject topdomain	2016-08-29 20:29:55	www.yahoo.com	yahoo
Reject topdomain	2016-08-29 20:14:28	www.google.com	google
Reject topdomain	2016-08-29 19:32:39	www.blogger.com	blogger
Reject topdomain	2016-08-29 15:52:33	www.baidu.com	baidu
Reject topdomain	2016-08-29 14:56:35	www.qq.com	qq
Reject topdomain	2016-08-29 14:05:52	google.com	google
Reject topdomain	2016-08-29 14:05:36	gmail.com	gmail
Reject topdomain	2016-08-29 13:31:59	samsung.com	samsung
Reject topdomain	2016-08-29 09:13:04	test.github.com	github
Reject topdomain	2016-08-29 00:54:06	www.google.com	google
Reject topdomain	2016-08-29 00:51:30	www.google.com	google
Reject topdomain	2016-08-29 00:51:09	google.com	google



Create Date	Domain	Keyword	Reaso
2016-08-31 04:41:20	onmicrosoft.com	microsoft	Reject|
2016-08-31 04:41:06	flaggerforcedev.onmicrosoft.com	microsoft	Reject|
2016-08-30 17:08:16	xevosnet.mail.onmicrosoft.com	microsoft	Reject|
2016-08-29 17:01:59	www.paypal-update-account-information.epizy.com	paypal	Reject| inform
2016-08-29 17:01:52	paypal-update-account-information.epizy.com	paypal	Reject|
2016-08-28 21:04:16	autodiscover.graeub.mail.onmicrosoft.com	microsoft	Reject|
2016-08-28 21:03:20	autodiscover.graeub.mail.onmicrosoft.com	microsoft	Reject|
2016-08-28 19:16:38	www.systemupdatepaypal.xyz	paypal	Reject|
2016-08-28 19:16:25	systemupdatepaypal.xyz	paypal	Reject|
2016-08-28 19:14:47	systemupdatepaypal.xyz	paypal	Reject|
2016-08-28 19:14:43	systemupdatepaypal.xyz	paypal	Reject|
2016-08-28 19:14:20	systemupdatepaypal.xyz	paypal	Reject|
2016-08-28 19:13:45	systemupdatepaypal.xyz	paypal	Reject|
2016-08-28 19:13:01	systemupdatepaypal.xyz	paypal	Reject|
2016-08-28 19:12:20	systemupdatepaypal.xyz	paypal	Reject|
2016-08-27 10:19:10	intlpaypallimit.com	paypal	Reject|
2016-08-27 10:19:10	intlpaypallimit.com	paypal	Reject|
2016-08-27 10:19:08	intlpaypallimit.com	paypal	Reject|
2016-08-27 10:19:08	intlpaypallimit.com	paypal	Reject|
2016-08-27 10:19:08	intlpaypallimit.com	paypal	Reject|
2016-08-27 10:19:07	intlpaypallimit.com	paypal	Reject|
2016-08-27 10:19:04	intlpaypallimit.com	paypal	Reject|
2016-08-26 22:29:46	paypal.update-your-account-information.keystonerocksupply.com	paypal	Reject| accoun
2016-08-26 17:03:27	secure.paypal.update.server.pligina.ru	paypal	Reject|
2016-08-26 17:00:09	paypal.secure.server.pligina.ru	paypal	Reject|
2016-08-26 17:00:02	paypal.secure.server.update.pligina.ru	paypal	Reject|
2016-08-26 16:59:51	paypal.secure.server.validation.pligina.ru	paypal	Reject|
2016-08-26 07:47:34	intlpaypallimit.com	paypal	Reject|
2016-08-26 07:47:33	intlpaypallimit.com	paypal	Reject|
2016-08-26 07:47:32	intlpaypallimit.com	paypal	Reject|
2016-08-26 07:47:31	intlpaypallimit.com	paypal	Reject|
2016-08-26 07:47:27	intlpaypallimit.com	paypal	Reject|
2016-08-26 07:04:30	googleoauth2.bitsiqhttech.com	google	Reject|

Figure 12

There are total 12 mis-issued certificates in this type, below is the detail info:



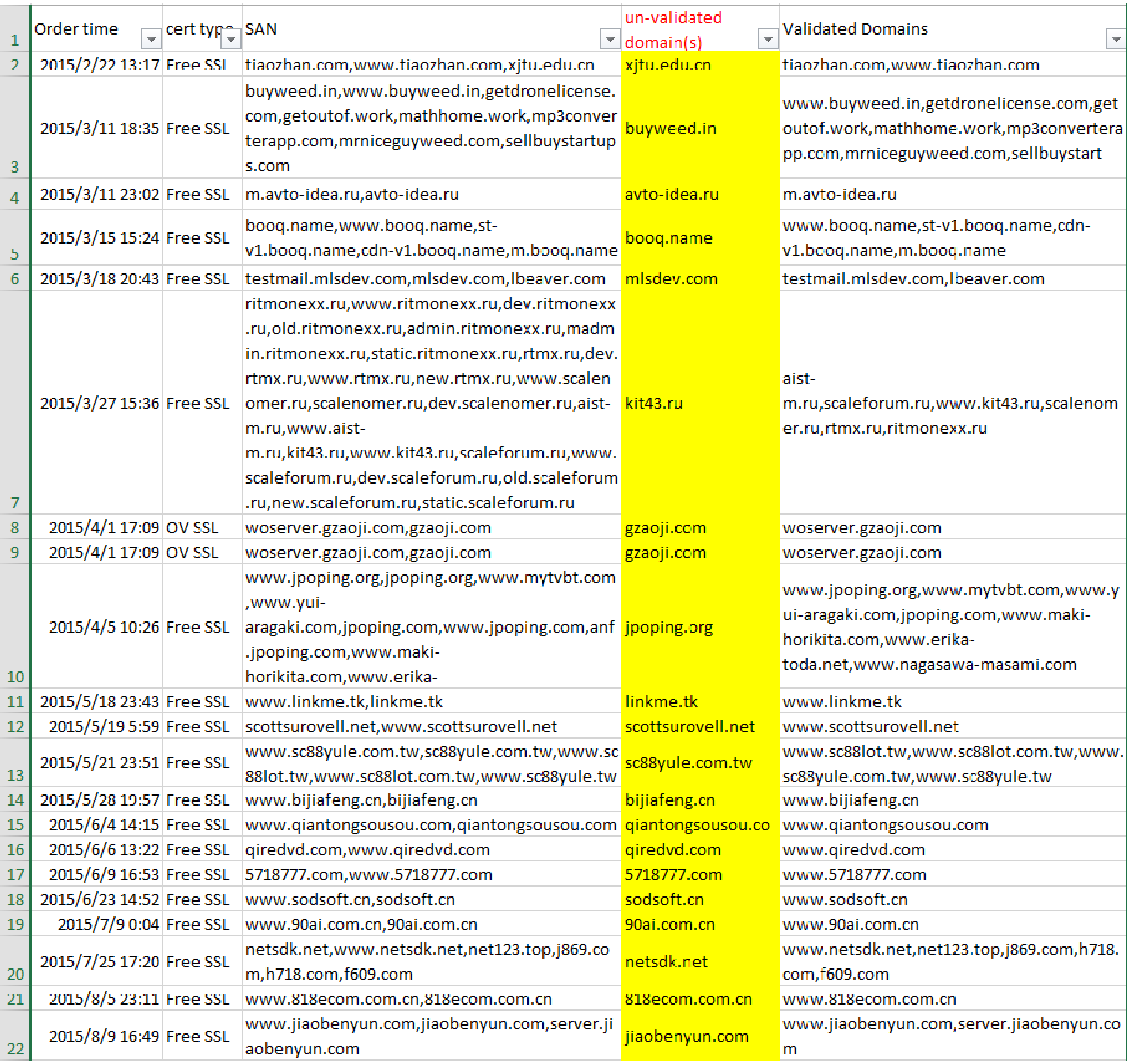
1	Order time	cert typ	SAN	un-validated domain(s	Validated Domains
2	2015/2/27 0:09	Free SSL	mail.netwi.ru,mail.idisk.su,mx.netwi.ru,mx.idisk.su	mx.idisk.su	netwi.ru
3	2015/3/1 11:50	Free SSL	dl.data800.com,dl.systemcn.com,api.data800.com,api.test.data800.com,api.systemcn.com,api.eggwifi.cn,api.test.systemcn.com,user.data800.com,user.systemcn.com,user.eggwifi.cn,svn.systemcn.com,svn1.systemcn.com,svn.data800.com,svn1.data800.com,svn1.eggwifi.cn,svn.eggwifi.cn,test.systemcn.com,test.data800.com,test.eggwifi.cn	api.eggwifi.cn,user.eggwifi.cn,test.eggwifi.cn	dl.data800.com,dl.systemcn.com,api.data800.com,api.test.data800.com,api.systemcn.com,api.test.systemcn.com,user.data800.com,user.systemcn.com,svn.systemcn.com,svn1.systemcn.com,svn.data800.com,svn1.data800.com,svn1.eggwifi.cn,svn.eggwifi.cn,test.systemcn.com,test.data800.com
4	2015/3/10 8:59	Free SSL	cloudapp.net,www.cloudapp.net,fl-repo.cloudapp.net	cloudapp.net,www.cloudapp.net	fl-repo.cloudapp.net
5	2015/3/10 23:01	Free SSL	suffit.org,www.suffit.org,static.suffit.org,dist.suffit.	suffit.org,www.suffit.or	static.suffit.org,dist.suffit.org
6	2015/3/11 16:51	Free SSL	neroanelli.no-ip.biz,trob.f3322.net	neroanelli.no-ip.biz	trob.f3322.net
7	2015/5/5 16:07	Free SSL	rederrik.ru,www.rederrik.ru,cash.rederrik.ru,app.rederrik.ru,xp.rederrik.ru	rederrik.ru,www.rederrik.ru,app.rederrik.ru,xp.r	cash.rederrik.ru
8	2015/5/11 13:45	Free SSL	dl.7r7z.com,dl.869v.com,dl.ke8u.com,dl.it376.com,dl.sh5y.com,down2.7r7z.com,down2.869v.com,down2.ke8u.com,down2.it376.com,down2.sh5y.com,xiazai2.7r7z.com,xiazai2.869v.com,xiazai2.ke8u.com,xiaz	dl.7r7z.com	dl2.7r7z.com,down2.7r7z.com,xiazai2.7r7z.com,dl.ke8u.com,down2.ke8u.com,xiazai2.ke8u.com,dl.sh5y.com,down2.sh5y.com,xiazai2.sh5y.com,dl.it376.com,d
9	2015/5/22 17:27	Free SSL	zentao.365jiating.com,365jiating.com,bug.365jiating	365jiating.com,bug.365ji	zentao.365jiating.com
10	2015/6/10 3:07	Free SSL	med.ucf.edu,www.ucf.edu	www.ucf.edu	med.ucf.edu
11	2015/6/10 11:47	Free SSL	schrauger.github.io,schrauger.github.com,github.io,github.com,www.github.io	github.io,www.github.io,github.com	schrauger.github.com,schrauger.github.io
12	2015/6/10 22:39	Free SSL	motorstoiclathe.github.io,www.github.io,github.io	www.github.io,github.io	motorstoiclathe.github.io
13	2015/6/12 15:22	OV SSL	open.wuji.com,itunes.wuji.com	open.wuji.com	itunes.wuji.com

Figure 13

2.3. Mis-added un-validated domain by system case

The another mis-issued case was adding additional domain rule bug. The rule is if you validated the domain: wosign.com, and you apply certificate for wosogn.com, then system will add a subdomain www.wosign.com in SAN for free, this is for the subscriber convenience that no any problem if the site visitor visit https://wosign.com and https://www.wosign.com. This is no any problem in domain control validation, but for website control validation method, it will have problem, the code engineer mis-understand this free add-domain rule, this is a code bug that we don't find even we revoked some mis-issued certificate, this bug is fixed completely at Aug. 10th, 2015 system update since we change the order procedure.

There are 21 mis-issued certificates in this type, below is the detail info, see Figure 14:



1	Order time	cert typ	SAN	un-validated domain(s)	Validated Domains
2	2015/2/22 13:17	Free SSL	tiaozhan.com,www.tiaozhan.com,xjtu.edu.cn	xjtu.edu.cn	tiaozhan.com,www.tiaozhan.com
3	2015/3/11 18:35	Free SSL	buyweed.in,www.buyweed.in,getdronelicense.com,getoutof.work,mathhome.work,mp3converterapp.com,mrniceguyweed.com,sellbuystartups.com	buyweed.in	www.buyweed.in,getdronelicense.com,getoutof.work,mathhome.work,mp3converterapp.com,mrniceguyweed.com,sellbuystart
4	2015/3/11 23:02	Free SSL	m.avto-idea.ru,avto-idea.ru	avto-idea.ru	m.avto-idea.ru
5	2015/3/15 15:24	Free SSL	booq.name,www.booq.name,st-v1.booq.name,cdn-v1.booq.name,m.booq.name	booq.name	www.booq.name,st-v1.booq.name,cdn-v1.booq.name,m.booq.name
6	2015/3/18 20:43	Free SSL	testmail.mlsdev.com,mlsdev.com,lbeaver.com	mlsdev.com	testmail.mlsdev.com,lbeaver.com
7	2015/3/27 15:36	Free SSL	ritmonexx.ru,www.ritmonexx.ru,dev.ritmonexx.ru,old.ritmonexx.ru,admin.ritmonexx.ru,madmin.ritmonexx.ru,static.ritmonexx.ru,rtmx.ru,dev.rtmx.ru,www.rtmx.ru,new.rtmx.ru,www.scalenomer.ru,scalenomer.ru,dev.scalenomer.ru,aist-m.ru,www.aist-m.ru,kit43.ru,www.kit43.ru,scaleforum.ru,www.scaleforum.ru,dev.scaleforum.ru,old.scaleforum.ru,new.scaleforum.ru,static.scaleforum.ru	kit43.ru	aist-m.ru,scaleforum.ru,www.kit43.ru,scalenomer.ru,rtmx.ru,ritmonexx.ru
8	2015/4/1 17:09	OV SSL	woserver.gzaoji.com,gzaoji.com	gzaoji.com	woserver.gzaoji.com
9	2015/4/1 17:09	OV SSL	woserver.gzaoji.com,gzaoji.com	gzaoji.com	woserver.gzaoji.com
10	2015/4/5 10:26	Free SSL	www.jpoping.org,jpoping.org,www.mytvbt.com,www.yui-aragaki.com,jpoping.com,www.jpoping.com,anf.jpoping.com,www.maki-horikita.com,www.erika-	jpoping.org	www.jpoping.org,www.mytvbt.com,www.yui-aragaki.com,jpoping.com,www.maki-horikita.com,www.erika-toda.net,www.nagasawa-masami.com
11	2015/5/18 23:43	Free SSL	www.linkme.tk,linkme.tk	linkme.tk	www.linkme.tk
12	2015/5/19 5:59	Free SSL	scottsurovell.net,www.scottsurovell.net	scottsurovell.net	www.scottsurovell.net
13	2015/5/21 23:51	Free SSL	www.sc88yule.com.tw,sc88yule.com.tw,www.sc88lot.tw,www.sc88lot.com.tw,www.sc88yule.tw	sc88yule.com.tw	www.sc88lot.tw,www.sc88lot.com.tw,www.sc88yule.com.tw,www.sc88yule.tw
14	2015/5/28 19:57	Free SSL	www.bijiafeng.cn,bijiafeng.cn	bijiafeng.cn	www.bijiafeng.cn
15	2015/6/4 14:15	Free SSL	www.qiantongsousou.com,qiantongsousou.com	qiantongsousou.co	www.qiantongsousou.com
16	2015/6/6 13:22	Free SSL	qiredvd.com,www.qiredvd.com	qiredvd.com	www.qiredvd.com
17	2015/6/9 16:53	Free SSL	5718777.com,www.5718777.com	5718777.com	www.5718777.com
18	2015/6/23 14:52	Free SSL	www.sodsoft.cn,sodsoft.cn	sodsoft.cn	www.sodsoft.cn
19	2015/7/9 0:04	Free SSL	www.90ai.com.cn,90ai.com.cn	90ai.com.cn	www.90ai.com.cn
20	2015/7/25 17:20	Free SSL	netsdk.net,www.netsdk.net,net123.top,j869.com,h718.com,f609.com	netsdk.net	www.netsdk.net,net123.top,j869.com,h718.com,f609.com
21	2015/8/5 23:11	Free SSL	www.818ecom.com.cn,818ecom.com.cn	818ecom.com.cn	www.818ecom.com.cn
22	2015/8/9 16:49	Free SSL	www.jiaobenyun.com,jiaobenyun.com,server.jiaobenyun.com	jiaobenyun.com	www.jiaobenyun.com,server.jiaobenyun.com

Figure 14

2.4 Impact Analytics

We classified this 33 misissuance certificate into two types: one type is we think this misissuance certificate is obviously not from the domain owner, we revoked this kind of certificates instantly after we know the misissuance. Another type is, this certificate is a normal order that the subscriber own this domain, it is our system bug fault to add a wrong related sub-domain or top domain to the certificate, in order to not interrupt those subscriber's website normal operation, we must notice those subscribers first, reissue a correct one for this subscriber, then revoke this mis-issued certificate.

Considering the website control validation method has potential risk, we have closed this method at

Aug. 27th 2016 even the BR allow this method. There are many famous Internet service providers provide subdomain to its customer, we can't add all of their domains to our Flag-Reject system. So we decided to close this validation method, only support domain control validation.

We posted all mis-issued 33 certificates to WoSign CT log server at Aug. 26th 2016 and Google CT log server at Sept. 03rd 2016 (some is in the Google CT server).
Here is the crt.sh link for all 33 certificates:
https://crt.sh/?id=7036355
https://crt.sh/?id=29805552
https://crt.sh/?id=7678955
https://crt.sh/?id=29805553
https://crt.sh/?id=29805554
https://crt.sh/?id=29805555
https://crt.sh/?id=29805556
https://crt.sh/?id=6798197
https://crt.sh/?id=29805558
https://crt.sh/?id=6798107
https://crt.sh/?id=29805559
https://crt.sh/?id=7728281
https://crt.sh/?id=29805560
https://crt.sh/?id=6639307
https://crt.sh/?id=29805561
https://crt.sh/?id=29805562
https://crt.sh/?id=6805650
https://crt.sh/?id=6739981
https://crt.sh/?id=7966229
https://crt.sh/?id=7094833
https://crt.sh/?id=29805563
https://crt.sh/?id=29805564
https://crt.sh/?id=29805565
https://crt.sh/?id=29805566
https://crt.sh/?id=29805567
https://crt.sh/?id=6843440
https://crt.sh/?id=29805568
https://crt.sh/?id=6999366
https://crt.sh/?id=29805569
https://crt.sh/?id=9534934
https://crt.sh/?id=29806448
https://crt.sh/?id=29813139
https://crt.sh/?id=29647048

3. Incident 2

3.1. Message from Mozilla

In July 2016, it became clear that there were some problems with the StartEncrypt automatic issuance service recently deployed by the CA StartCom. As well as other problems it had, which are outside the scope of this discussion, changing a simple API parameter in the POST request on the submission page changed the root certificate to which the resulting certificate chained up. The value "2" made a certificate signed by "StartCom Class 1 DV Server CA", "1" selected "WoSign CA Free SSL Certificate G2" and "0" selected "CA 沃通根证书", another root certificate owned by WoSign and trusted by Firefox.

Using the value "1" led to a certificate which had a notBefore date (usage start date) of 20th December 2015, and which was signed using the SHA-1 checksum algorithm.

** The issuance of certificates using SHA-1 has been banned by the Baseline Requirements since January 1st, 2016. Browsers, including Firefox, planned to enforce this by not trusting certs with a notBefore date after that date, but in the case of Firefox the fix had to be backed out due to web compatibility issues. However, we are considering how/when to reintroduce it, and CAs presumably know this.*

** The issuance of backdated certificates is not forbidden, but is listed in Mozilla's list of Problematic Practices. It says "Minor tweaking for technical compatibility reasons is accepted, but backdating certificates in order to avoid some deadline or code-enforced restriction is not."*

** WoSign deny that their code backdated the certificates in order to avoid browser-based restrictions - they say "this date is the day we stop to use this code". If that is true, it is not clear to us how StartCom came to deploy WoSign code that WoSign itself had abandoned.*

** It seems clear from publicly available information that StartCom's issuance systems are linked to WoSign's issuance systems in some way.*
Nevertheless, it should not have been possible for an application for a cert from StartCom to produce a cert signed by WoSign.

** This misissuance incident was not reported to Mozilla by WoSign as it should have been.*

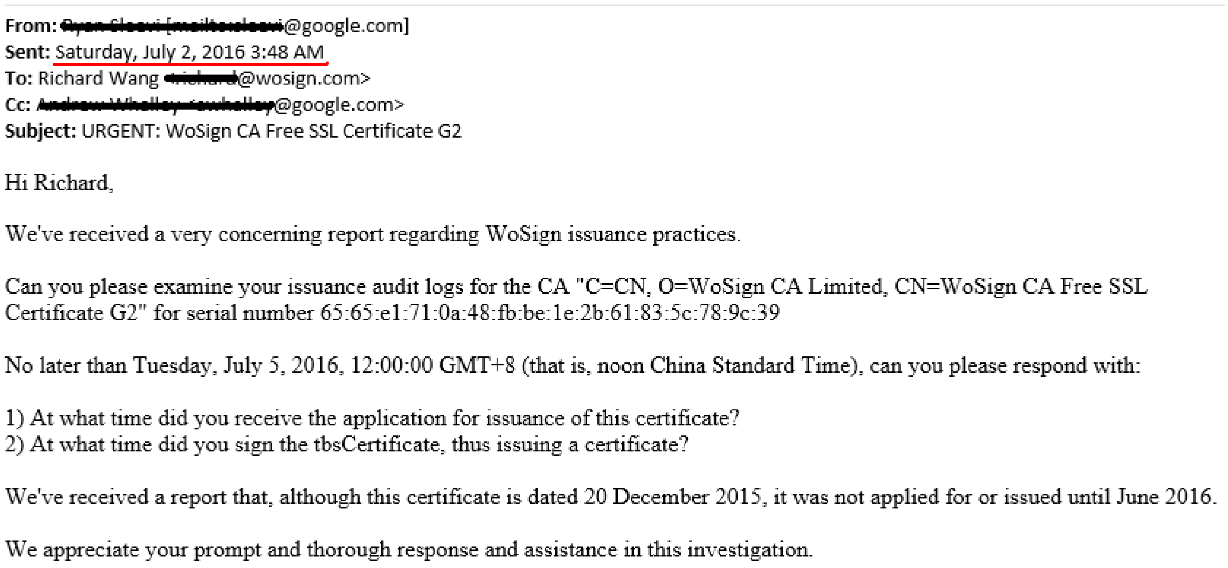
3.2. Incident Response

We declared this big in Bugzilla: https://bugzilla.mozilla.org/show_bug.cgi?id=1293366, this is not the case that we want to issue backdated SAH1 certificate intentionally, this is a bug that used by the test company to issued two certificates only. StartCom and WoSign used the same auto-generation script, set different parameter to go to different CA API URL. Now StartCom and WoSign all decided to use ACME protocol that it will support this case -- one same client software can be used to get certificate from different CA, just define the CA parameter.

We revoked this two mis-issued SHA1 certificate instantly after getting report at June 30, 2016. And

we deleted this bug code in API instantly, and StartCom stopped StartEncrypt service at July 4th. Here is the two mis-issued SHA1 certificate link in crt.sh:
https://crt.sh/?id=30741722
https://crt.sh/?id=30741724

We got the report from Google on **July 2nd 2016 3:48AM**, see Figure 15, and find this case in our system and reply Google email at **July 2nd, 2016 11:20AM** (this is the **Saturday**), see below screenshot (Figure 16):



From: [redacted]@google.com]
Sent: Saturday, July 2, 2016 3:48 AM
To: Richard Wang [redacted]@wosign.com>
Cc: [redacted]@google.com>
Subject: URGENT: WoSign CA Free SSL Certificate G2

Hi Richard,

We've received a very concerning report regarding WoSign issuance practices.

Can you please examine your issuance audit logs for the CA "C=CN, O=WoSign CA Limited, CN=WoSign CA Free SSL Certificate G2" for serial number 65:65:e1:71:0a:48:fb:be:1e:2b:61:83:5c:78:9c:39

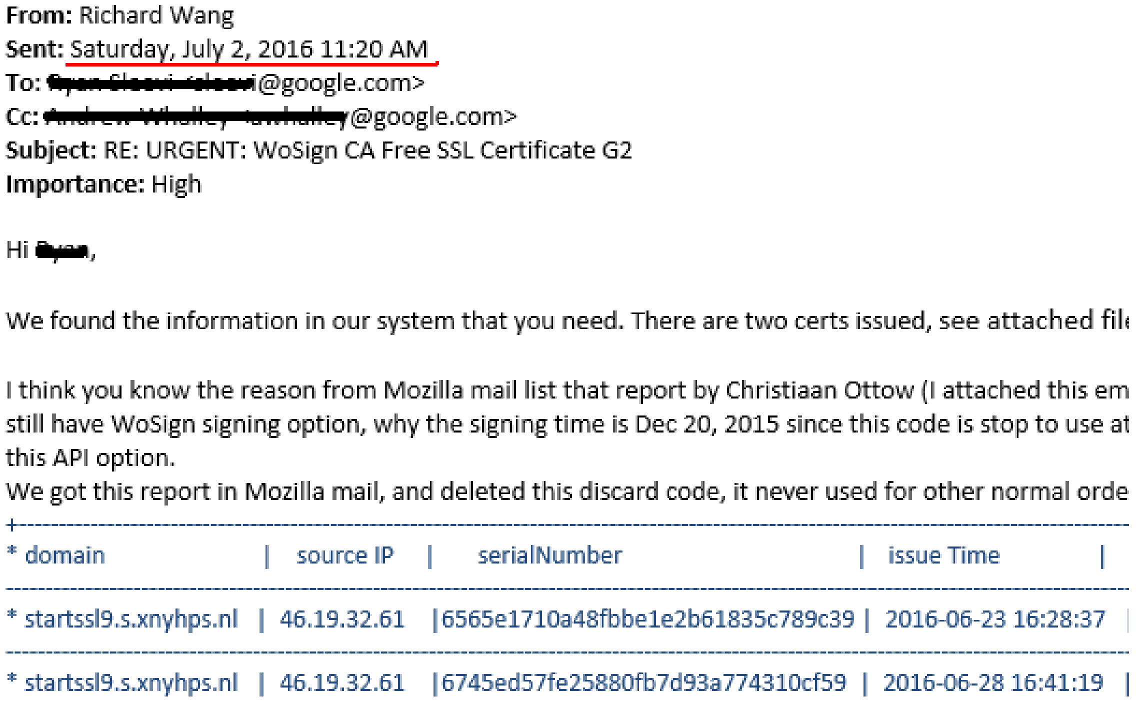
No later than Tuesday, July 5, 2016, 12:00:00 GMT+8 (that is, noon China Standard Time), can you please respond with:

1) At what time did you receive the application for issuance of this certificate?
2) At what time did you sign the tbsCertificate, thus issuing a certificate?

We've received a report that, although this certificate is dated 20 December 2015, it was not applied for or issued until June 2016.

We appreciate your prompt and thorough response and assistance in this investigation.

Figure 15



From: Richard Wang
Sent: Saturday, July 2, 2016 11:20 AM
To: [redacted]@google.com>
Cc: [redacted]@google.com>
Subject: RE: URGENT: WoSign CA Free SSL Certificate G2
Importance: High

Hi [redacted],

We found the information in our system that you need. There are two certs issued, see attached fil

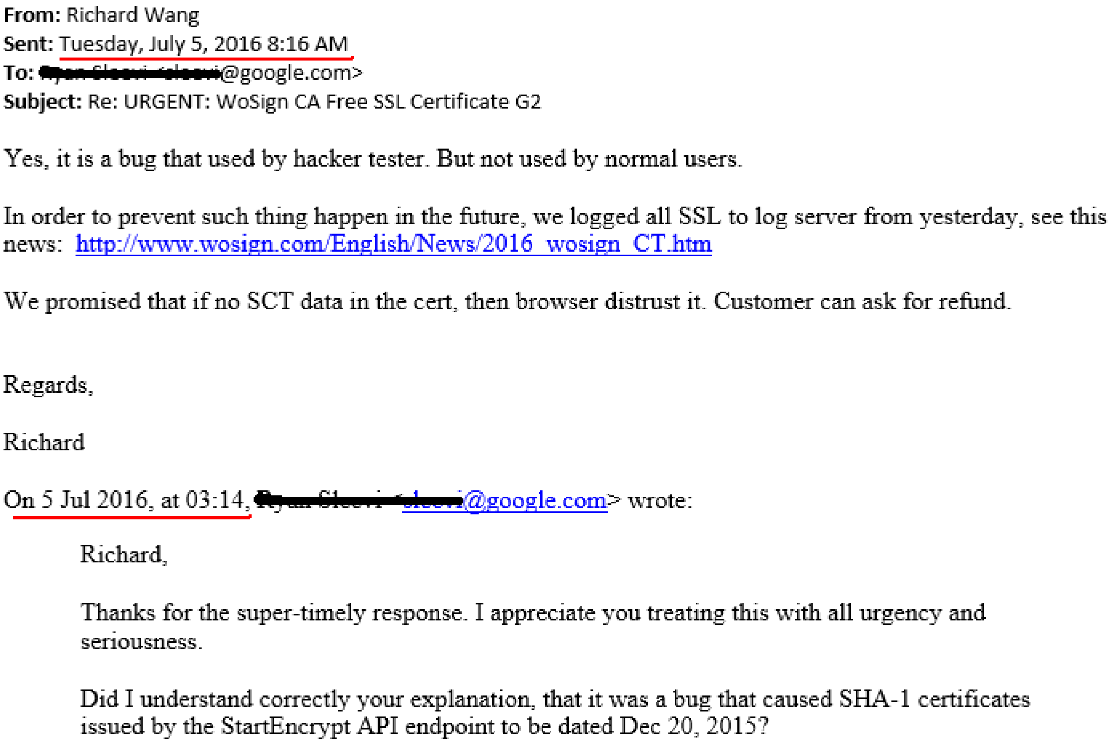
I think you know the reason from Mozilla mail list that report by Christiaan Ottow (I attached this em
still have WoSign signing option, why the signing time is Dec 20, 2015 since this code is stop to use at
this API option.
We got this report in Mozilla mail, and deleted this discard code, it never used for other normal orde

```
+----------------------------------------------------------------------------------------------------
* domain                 |  source IP  |   serialNumber                        |  issue Time         |
-----------------------------------------------------------------------------------------------------
* startssl9.s.xnyhps.nl  |  46.19.32.61 |6565e1710a48fbbe1e2b61835c789c39 |  2016-06-23 16:28:37 |
-----------------------------------------------------------------------------------------------------
* startssl9.s.xnyhps.nl  |  46.19.32.61 |6745ed57fe25880fb7d93a774310cf59 |  2016-06-28 16:41:19 |
```

Figure 16

In order to be transparency, WoSign decided to post all SSL certificates to Google CT log server and release this news: https://www.wosign.com/english/News/2016_wosign_CT.htm at **July 4** (**Monday**).

And we got replied from Google at **July 5 03:14AM**, replied to Google to declare it is a bug. And tell Google we decided to log all SSL certificate from July 4th and released news.



From: Richard Wang
Sent: Tuesday, July 5, 2016 8:16 AM
To: [redacted]@google.com>
Subject: Re: URGENT: WoSign CA Free SSL Certificate G2

Yes, it is a bug that used by hacker tester. But not used by normal users.

In order to prevent such thing happen in the future, we logged all SSL to log server from yesterday, see this news: http://www.wosign.com/English/News/2016_wosign_CT.htm

We promised that if no SCT data in the cert, then browser distrust it. Customer can ask for refund.

Regards,

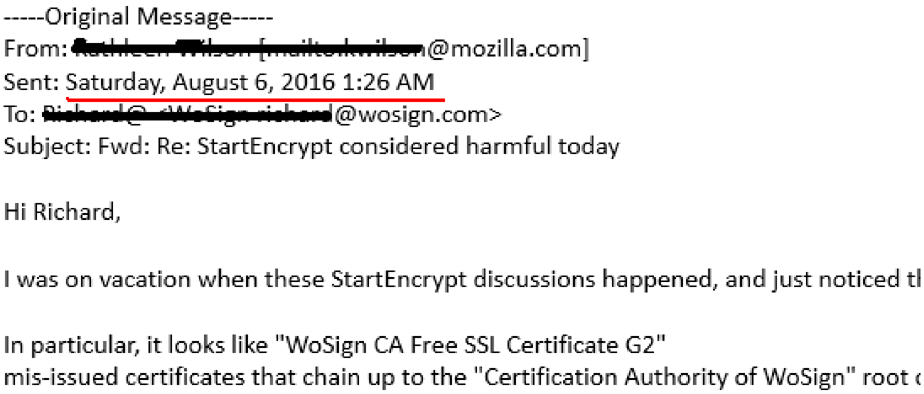
Richard

On 5 Jul 2016, at 03:14, [redacted]@google.com> wrote:

> Richard,
>
> Thanks for the super-timely response. I appreciate you treating this with all urgency and seriousness.
>
> Did I understand correctly your explanation, that it was a bug that caused SHA-1 certificates issued by the StartEncrypt API endpoint to be dated Dec 20, 2015?

Figure 17

And we also got email from Mozilla at **Aug. 6, 2016 1:26 AM** (this is the **Saturday**), see below screenshot:



-----Original Message-----
From: [redacted]@mozilla.com]
Sent: Saturday, August 6, 2016 1:26 AM
To: [redacted]@wosign.com>
Subject: Fwd: Re: StartEncrypt considered harmful today

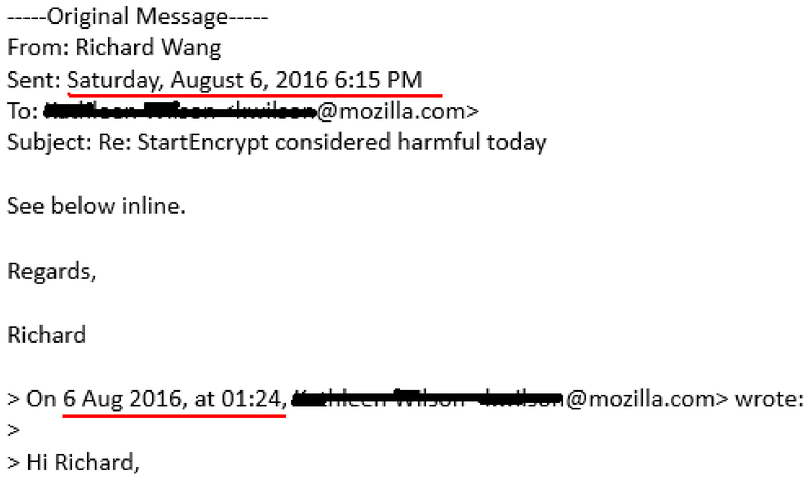
Hi Richard,

I was on vacation when these StartEncrypt discussions happened, and just noticed tl

In particular, it looks like "WoSign CA Free SSL Certificate G2"
mis-issued certificates that chain up to the "Certification Authority of WoSign" root (

Figure 18

And Richard replied Mozilla email at **Aug. 6, 2015 6:15 PM** (Saturday), and explained the situation that same as the reply to Google:



-----Original Message-----
From: Richard Wang
Sent: Saturday, August 6, 2016 6:15 PM
To: [redacted]@mozilla.com>
Subject: Re: StartEncrypt considered harmful today

See below inline.

Regards,

Richard

> On 6 Aug 2016, at 01:24, [redacted]@mozilla.com> wrote:
>
> Hi Richard,

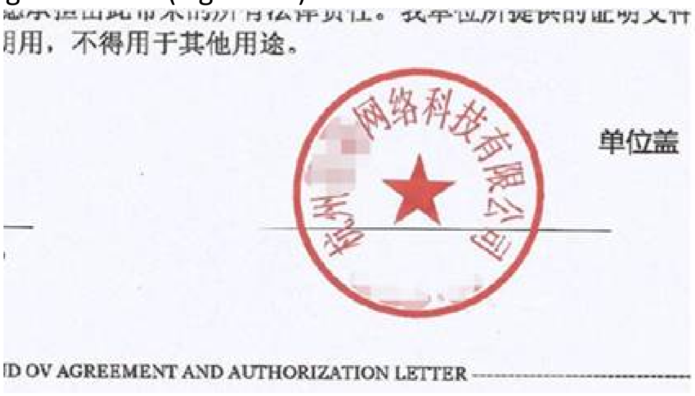
Figure 19

Summary

WoSign started CA business since 2005 as GeoTrust reseller, then we are reseller of VeriSign and Thawte after VeriSign acquired GeoTrust, and the reseller of Trust Center, Comodo etc. We learn many from these CA Giants. WoSign launched its own root CA since 2011, we passed the WebTrust audit since 2012 by E&Y, we know China market and we invented some good validation method to prevent fraud that we can share this to CA industry, we try our best to do the validation, and we also know system security is the most important thing for our business and do it seriously.

1. For identity validation, the CA normal phone call validation is no any meaning in China since China don't have reliable phone directory, and many company office's phone number is owned by the building owner, not the company. So we used the bank transfer verification that it is very reliable, subscriber MUST transfer the payment from his personal bank account (Class 2) or from his company bank account (Class 3 and Class 4) to WoSign company bank account, no any fraud subscriber can fake this way together with the authorization letter;

2. China use Company Seal instead of hand signature, we identified many Photoshop-made business license and company seal, it is very hard to identify it out as fraud one if you don't understand Chinese and Chinese culture, see below screenshot, this is a PhotoShop-made, fake one! It is not genuine one(Figure 20):



用用，不得用于其他用途。

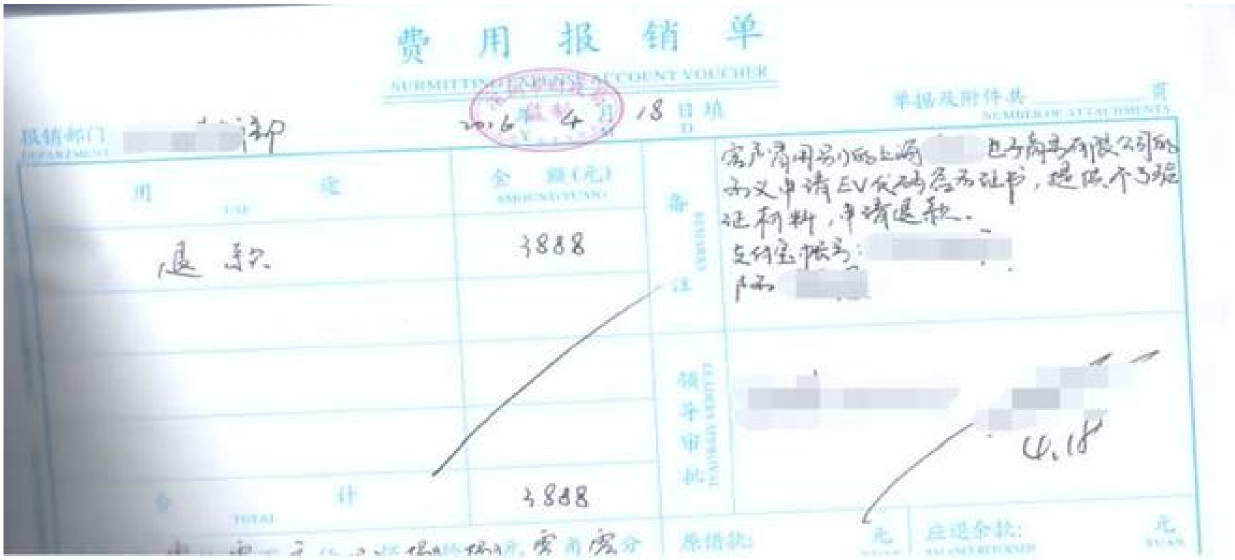
网络科技有限公司

单位盖

D OV AGREEMENT AND AUTHORIZATION LETTER

Figure 20

3. If we find this subscriber used the fraud business license with fraud seal, we reject their order and refund the money, see Figure 21, this is the internal refund approval document screenshot, this guy want to buy EV code signing using a fraud document, but rejected by our validation team.



费用报销单

SUBMITTING EXPENSE ACCOUNT VOUCHER

报销部门 DEPARTMENT [redacted]部

2016年4月18日填

单据及附件共 页 NUMBER OF ATTACHMENTS

用途 USE	金额(元) AMOUNT(YUAN)	备注 REMARKS
退款	3888	客户采用另外的上海[redacted]电子商务有限公司的名义申请EV代码签名证书，提供了不实验证材料，申请退款。 支付宝账号：[redacted] 户名[redacted]
		领导审批 LEADER'S APPROVAL [redacted] 4.18
合计 TOTAL	3888	原借款： 元 YUAN 应退余款： 元 YUAN BALANCE REFUND

Figure 21

As our promised in the Mozilla-Dev-Security-Policy mail list reply, we posted all 2015 issued SSL certificates to Google log server and WoSign log server, and till now we are still checking our system to try to find if we missed any certificate that not posted, we even posted the SSL certificate issued at Dec 31, 2014 and Jan. 1st 2016 in case of the database time zone difference problem. And we plan to post all issued SSL certificate in 2016 before July 5th for full transparency, but this need time since the related team is busy with the investigation and report.

Finally, we are very sorry for the incidents had not been reported to Mozilla as it should have been, we just responded to the inquiry from browser companies.
We also learned that we need to invest more on the quality control, try our best to find out the vulnerabilities from any unusual case and incident.

Please feel free to contact Richard Wang at richard@wosign.com if you have any questions, thanks.

Sincerely yours,

Richard Wang,

CEO
WoSign CA Limited