The MCS Incident and Its Consequences for CNNIC

Outline

1. Background on CNNIC and the MCS Incident

China Internet Network Information Center (CNNIC), a non-profit organization administered by Cyberspace Administration of China (CAC), operates the “CNNIC Root” and “China Internet Network Information Center EV Certificates Root” certificates that are included in Mozilla’s root store, and used to issue certificates to organizations and the general public.

This document is an analysis of the status of the CNNIC roots in Mozilla’s root store, triggered by a recent incident involving the issuance of a certificate to Mideast Communication Systems (MCS), an Egyptian company.

1.1. MCS Incident

CNNIC issued an unconstrained intermediate certificate (a certificate capable of issuing other certificates, including those for any website on the Internet) under the “CNNIC Root”. This certificate was labeled as a test certificate and had a 23 day validity, expiring April 3, 2015. The holder of the private key for this certificate was MCS. MCS used this certificate in a firewall device which performed SSL MITM, and a user inside their network accessed servers on the Internet, causing the firewall to dynamically issue certificates for domains that this customer did not own or control (e.g. Google-owned domains).

CNNIC has affirmed that their customer, MCS, did not have a Certificate Practice Statement (CPS) developed, and so did not have an approved Key Generation Script (which would have

directed the creation of the intermediate in an appropriate fashion), did not have a Point-in-Time Readiness Assessment (which would have scrutinised the conditions in which it was stored), and lacked any form of controls beyond that of contractual agreement.

MCS has affirmed that their plan was to do some testing with this certificate before building their secure system for hosting a future longer-lived intermediate. They explained that CNNIC did not give them any guidance or instructions on how to securely hold or manage an unconstrained intermediate certificate, and that they used what they thought was their most secure system to hold the certificate private key, which happened to be a firewall with SSL interception capability.

1.2. Violation of CNNIC Certificate Policy and Certificate Practice Statement

Every CA is required to have a Certificate Policy and Certification Practice Statement (CPS) which explains how they run their CA. A CA's inclusion in the root program is based on their CP and CPS; they are the covenant that the CA makes with the community about how they will operate.

CNNIC's current CPS (v.3.03):

- Does not provide for or describe the issuance procedures for subordinate CA certificates, test or otherwise. The closest approximation is Section 2.2.10, which describes CNNIC pursuing cross-certification for their own root, not the use of CNNIC's PKI to cross-certify.
- States in Section 6.2.3 that "The private keys of the root certificates and intermediate root certificates of CNNIC Trusted Network Service Center are not entrusted to another agency, nor does CNNIC Trusted Network Service Center accept the entrustment from any certificate applicant to keep signature private keys." Two possible interpretations of this exist:
    - this is a reaffirmation that subordinate CA keys are not issued (consistent with the rest of the CPS, and based upon "entrusted to another agency" referring to MCS); or
    - they only control the private keys detailed within the CPS itself.
- States in Section 7.1.2 that the profile for issued certificates will have a CA=FALSE, (though "basicConstraints" is mistranslated as "Basic Restriction") by saying "Subject Type = End Entity"; in other words, they don't issue intermediate certificates to third parties.

Therefore, according to their own CPS, CNNIC should not have issued this certificate. CNNIC have argued in discussion that this certificate was just for testing purposes, and they were planning to make the necessary changes at the time of their next audit in April 2015.

1.3. Violation of Mozilla Policy

Sections 8 through 10 of Mozilla's CA Certificate Inclusion Policy and Section 17 of the Baseline Requirements (BRs - a CAB Forum document which our policy requires all CAs to comply with) require that all certificates "capable of being used to issue new certificates" MUST either be **technically constrained** (as described in BR Section 9.7) or **disclosed and audited** in line with Mozilla's CA Certificate Inclusion Policy and all of the requirements of BR Section 17.

> *10. ... All certificates that are capable of being used to issue new certificates, that are not technically constrained, and that directly or transitively chain to a certificate included in Mozilla's CA Certificate Program MUST be audited in accordance with Mozilla's CA Certificate Policy and MUST be publicly disclosed by the CA that has their certificate included in Mozilla's CA Certificate Program. The CA with a certificate included in Mozilla's CA Certificate Program MUST disclose this information before any such subordinate CA is allowed to issue certificates. (link)*

In other words, intermediate CAs must be either constrained so they can't hurt the wider web, or made known to the web and have their storage and use audited, to make sure they are being used appropriately. This requirement has been in place since version 2.1 of the policy, and came into full effect for all CAs and all intermediate certificates in May 2014.

Prior to the issuance of an unconstrained intermediate certificate such as the MCS certificate, CNNIC should have ensured that the subordinate CA's environment met CNNIC's documented practices and policies, ensured that the keys were generated in a physically secured environment, ensured that the subordinate CA had appropriate certificate policy and practice documentation, and had a Point-in-Time Readiness Assessment.

None of these things happened. Therefore, according to Mozilla policy and the Baseline Requirements, CNNIC should not have issued this certificate. CNNIC have argued in discussion that, for a testing certificate, contractual controls (restricting the cert to be used for domains MCS own or control) alone were sufficient.

Given the nature of these violations, there are no guarantees that these misissued certificates would have been detected by an audit. CNNIC limited the certificate validity to 23 days, none of which were during an audit period, so such certificates could have only been detected by sampling during the next audit period. As BR Section 17.8 only dictates a quarterly audit of 1 cert or 3% of issued certs, there is a significant probability that this certificate would not have shown up. Had it shown up, the fact that it has expired may, for many auditors, prevent a qualified finding from being issued, thus preventing from Mozilla being notified.

1.4. CNNIC Acknowledgements of Mozilla Policies

Mozilla regularly issues “CA Communications” to all CAs in our program to inform them of changes and ask them for information. Each CA is required to respond to the communication.

Feb 2012:

> *As a CA in Mozilla’s root program you are ultimately responsible for certificates issued by you and any intermediate CAs that chain up to your roots. After April 27, 2012, if it is found that a subordinate CA is being used for MITM, we will take action to mitigate, including and up to removing the corresponding root certificate. Based on Mozilla’s assessment, we may also remove any of your other root certificates, and root certificates from other organizations that cross-sign your certificates. (link)*

CNNIC responded as follows (relevant parts given):

> 1, We reviewed all subordinate CAs of CNNIC, none of them are used for MITM and Traffic Management.
> 2, CNNIC CA never issued subCA to third parties.
> …
> 5, I will review the "Baseline Requirements". And I will update our operation and documentation as needed to meet Baseline Requirements in the forum before July 1, 2012.

Jan 2013:

> *Due to the recent incident in which a mis-issued intermediate certificate was found, we are concerned that CAs may have responded to our last communication based on their policies, rather than checking their certificate databases. Therefore, we request that you scan your certificate database and inform Mozilla if you find any un-expired intermediate certificates in your CA hierarchy that should not be trusted. In your reply, please attach all such intermediate certificates, even if you have already revoked them. (link)*

CNNIC responded as follows (relevant parts given):

> 2, a) Our CA operations conform to the CA/Browser Forum’s Baseline Requirements for issuance of SSL certificates, and our next audit will include verification of this conformance.
> 3, a) We have scanned our certificate database, and confirm that there are no un-expired intermediate certificates in our CA hierarchy that should not be trusted. We

have also checked our certificate database to confirm that all of the non-expired certificates have been issued in accordance with the listed practices.

July 2013:

> *2) Review your CA operations and customers to ensure that there are no certificates chaining up to your trust anchors that are included in Mozilla's program that may be used for MITM or "traffic management" of domain names or IP addresses that the certificate holder does not own or control. Mozilla's CA Certificate Enforcement Policy has been updated to make it clear that Mozilla will not tolerate this use of publicly trusted certificates.*
>
> *Please respond with: "We have reviewed Mozilla's updated CA Certificate Enforcement Policy and understand that knowing or intentional mis-issuance of a certificate is expressly against Mozilla's CA Certificate Policy and could result in removal of all of our certificates from Mozilla's products." (link)*

CNNIC responded as follows (relevant parts given):

> 2) We have reviewed Mozilla's updated CA Certificate Enforcement Policy and understand that knowing or intentional mis-issuance of a certificate is expressly against Mozilla's CA Certificate Policy and could result in removal of all of our certificates from Mozilla's products.
> 5) We have no intermediate certificates revoked currently.

May 2014:

> *5) Send Mozilla information about your publicly disclosed subordinate CA certificates that chain up to certificates in Mozilla's CA program, as per Items #8, 9, and 10 of Mozilla's CA Certificate Inclusion Policy.*
>
> *Please provide a URL to a web page or a Bugzilla Bug Number that lists all of your publicly disclosed subordinate CA certificates that chain up to certificates in Mozilla's CA program, and contains the required information according to section 10 of Mozilla's CA Certificate Inclusion Policy. If you decide to use the mozilla.org Bugzilla system to provide this information, then file the bug against the "CA Certificates" component of the "mozilla.org" product. (link)*

CNNIC responded as follows (relevant parts given):

> 5) The following is the URL link to our 3 sub CA linked to our root which included in Mozilla. The 3 sub-CA are all internal sub-ca and operated by CNNIC.
> https://evdemo.cnnic.cn;

https://mail.cnnic.cn;
https://mail.id110.cn;
A) All subordinate CA certificates chaining up to our certificates in Mozilla's CA program are either disclosed as requested above, or are technically constrained according to section 9 of Mozilla's CA Certificate Inclusion Policy.

All of these responses together show that CNNIC was aware of the fact that MITM is forbidden. In fact, this was reflected in their contract with MCS, which forbids MCS to issue for any domains other than those owned and controlled by MCS.

The response from May 2014 shows that CNNIC was aware of the fact that intermediate certificates must be technically constrained or disclosed and audited. The MCS certificate was not technically constrained, and it had neither been disclosed nor audited.

2. Remedial Action

Based on our review of the details, we believe that the intermediate certificate was mis-issued. That certificate has already been marked as revoked using the OneCRL facility, which makes it untrusted in Firefox 37 (the current release) and later.

With regard to CNNIC's root certificates, several courses of additional action have been considered, with the following information being taken into account.

2.1. Relevant Mozilla Policy and Other Guidance

According to Mozilla's wiki page Maintaining Confidence in Root Certificates, the response to a CA mis-issuing an intermediate certificate at minimum should include distrusting the intermediate certificate, and doing further analysis to consider distrusting the root certificate or all of the root certificates owned by that CA.

> *Problem: CA mis-issued a small number of intermediate certificates that they can enumerate*
>
> - *Immediate Minimum Response: Actively distrust the intermediate certificates, and push out an update to all Mozilla products.*
> - *Depending on the situation, also consider distrusting the root certificate or all of the root certificates owned by that CA.*

According to Mozilla's CA Certificate Enforcement Policy, Mozilla may, at its sole discretion, disable or remove a certificate at any time and for any reason.

> *2. Mozilla may, at its sole discretion, disable (partially or fully) or remove a certificate at any time and for any reason. Mozilla will disable or remove a certificate if the CA demonstrates ongoing or egregious practices that do not maintain the level of service that was established in the Inclusion Section of the Mozilla CA Certificate Policy or that*

do not comply with the requirements of the Maintenance Section of the Mozilla CA Certificate Policy. (link)

Ongoing or Egregious Practices

Some key words in the Enforcement Policy quoted above, relating to disablement or removal, are “ongoing or egregious practices”.

The word “ongoing” indicates that the CA has made more than one significant mistake, or has repeatedly made the same significant mistake. The significance or severity of the mistakes, in regards to the potential impact to the safety of our end users, are taken into account when considering the number of mistakes that are allowed before action, such as partial or full removal, will be taken.

The word “egregious” indicates that the CA has made blatant or conspicuously bad or flagrant mistakes, with potentially serious impact to the safety of our end users.

As examples of what this means, Mozilla considers the following to be egregious practices:

- Issuing an unconstrained intermediate certificate to an external third party who does not have documented PKI practices and whose systems and practices have not been vetted by the CA to ensure that the subordinate CA is in compliance with the CA’s policies.
- Issuing an unconstrained intermediate certificate to an external third party when the CA’s documented policies do not allow this, and do not specify the expectations and required practices of external subordinate CAs.
- Issuing certificates in a manner that is not consistent with the CA’s CPS and puts the safety of end-users at risk.
- Knowingly issuing certificates without the knowledge of the entities whose information is referenced in the certificates.
- Knowingly issuing certificates that appear to be intended for fraudulent use.
- Lack of logging and controls such that, after a breach which results in the misissuance of certificates, it is not possible to determine how many certificates were misissued and what information they contained.
- Mis-issuing an unknown number of un-enumerated intermediate certificates.

2.2. Incidents Comparable to the MCS Incident

There are a number of intermediate-used-for-MITM cases which are similar in some ways to this one. The relevant facts of those cases are outlined here.

Trustwave (February 2012)

Trustwave is a commercial CA which knowingly issued two unconstrained intermediate certs to a 3rd party corporation for the purposes of MITM on their internal network, and the 3rd party deployed it in line with its intended purpose.

Mozilla's response to this incident was to issue an update blacklisting the two certs, and send a CA Communication clarifying that this practice was unacceptable. Mozilla gave all CAs 2 months to identify and revoke such intermediates, and tell us about it. No specific action was taken against Trustwave.

Comparing with the current case: unlike with Trustwave, CNNIC did not issue the cert for the purposes of MITM, but it was used for that purpose in violation of contract.

TurkTrust (January 2013)

TurkTrust is a commercial CA which mistakenly issued unconstrained intermediate certs when it meant to issue end-entity certs, and one of those was subsequently used for MITM. It was never determined how the target organization worked out that this was even possible, or whether it was some incredible fluke that the cert they loaded into their MITM device just happened to be one which worked. Given that the CA didn't intend to issue an intermediate, whether they "allowed" MITM is a moot point.

Mozilla's response to this incident was to issue an update blacklisting the two certs and to put TurkTrust's request for inclusion of a new root with EV status on hold for approximately 5 months, while they had an additional audit done.

Comparing with the current case: in this case, CNNIC intentionally issued the intermediate; it was not an error.

ANSSI (December 2013)

ANSSI is the CA of the French Government, which issued an intermediate to another part of the same organization; that part decided to do SSL MITM for the purpose of blocking access to certain websites they saw as unsafe, and so issued themselves a further intermediate and loaded it into their firewall. This was a violation of root policy, and as soon as the root found out, they revoked and destroyed the special intermediate which had been issued for this purpose.

Mozilla's response to this incident was to issue an update blacklisting the cert and to constrain ANSSI's roots to issuing for the TLDs corresponding to the territories over which the French government has jurisdiction - .fr primarily, but also 12 other TLDs corresponding to French overseas departments and territories (e.g. .gp for Guadeloupe).

Comparing with the current case: CNNIC issued to a different organization rather than another part of the same organization. The two incidents are similar in that a downstream certificate holder used the cert in violation of policy/contract.

2.3. Distrusting New CNNIC Certificates

The Mozilla CA team believes that CNNIC's actions amount to egregious behaviour, and the violations of policy are greater in severity than those in previous incidents. CNNIC's decision to violate their own CPS is especially serious, and raises concerns that go beyond the immediate scope of the mis-issued intermediate certificate.

After public discussion, and careful consideration of the impact and consequences of various possible forms of additional action, we are planning to change Firefox's certificate validation code such that it refuses to trust any certificate issued by a CNNIC root with a notBefore date on or after 1 April 2015. This change will persist until CNNIC has re-completed the full application process for re-inclusion in Mozilla's root store (should they choose to re-apply), possibly including some additional steps that the community may require as a result of this incident. While CNNIC's re-application process is in progress, they will remain in the root store so that old certificates can still be verified. As long as they are in this state, they will be held to the normal standards of the root program with regard to audits, etc.

This plan relies on CNNIC accurately reflecting issuance times in the notBefore field. We will be asking CNNIC for a comprehensive list of their currently-valid certificates, and publishing it. After the list has been provided, if a certificate not on the list, dated before 1 April 2015, is detected on the public internet, we reserve the right to take further action.

We believe that this response is consistent with Mozilla policy and other guidance, and is one which we could apply to any other CA in the same situation.

Credits: Thanks to Google for informing us about the MCS misissuance, to Ryan Sleevi for his initial public analysis of the situation, and to Peter Bowen for suggesting a date-based restriction.