Dossier: automated certificate report generation for Bugzilla

Open-Source Software

https://github.com/digicert/dossier

Background

- Most incidents involve certificates
- Affected certificates need to be disclosed in incident reports
- CCADB Incident Reporting Guidelines has an explicit format for reporting certificate data
  - Consistency and specificity is good
  - But it’s also a challenge to generate manually

Can we automate it all?

- We can automatically extract certificate information (subject, issuer, serial number, etc.)
- Thanks to CCADB reports, we also have:
  - CA information, including PEMs
  - CRL URIs

We have the technology

- With these ingredients, we can build a tool that is provided the affected certificates, the incident discovery time, and the revocation window (24 hours, 5 days, or 7 days), and can then:
  - Extract certificate information (serial number, issuer, etc.)
  - Fetch CRL-based revocation data
    - Both full CRLs and partitioned CRLs
  - Determine the revocation status (expired, not revoked, revoked timely, or delayed revocation)
- And produce a report in the required format
  - “Full” report when there are less than 10,000 certificates
  - crt.sh link report when there are more
  - Redact S/MIME subject information

Dossier

- Command line tool to generate certificate reports in the format specified by the CCADB Incident Reporting Guidelines
- Automatically does all the things listed in slide 4
- Supports PEM- and DER-encoded certificate files, CSV files, and ZIP archives

Where to get it

- Open Source from DigiCert
- Available as a Python package on PyPi: https://pypi.org/project/cert-dossier/
- Source code on Github: https://github.com/digicert/dossier

We think this tool can be of use to CAs, and we intend for it to be an ecosystem resource

- Your ideas and PRs are welcome to improve the tool

Thank you!