Mozilla News

CA/B Forum F2F, Meeting 62 in Bergamo, Italy
May 28, 2024

Ben Wilson

Link to Previous Mozilla February 2024 Face-to-Face briefing - https://cabforum.org/2024/02/26/minutes-of-the-f2f-61-meeting-in-new-delhi-india-february-26-27-2024/2-February-2024-Mozilla%20Browser%20News.pdf

CA Compliance - https://wiki.mozilla.org/CA/Incident_Dashboard
Current open bugs can be found in the Incident Dashboard (currently 90 are open).

Bugzilla incidents that were open at any time between January 1, 2024, and May 20, 2024, (total of 136) have been categorized as follows:

Type of Incident	Count
Audit Delays and Findings	**6**
CA Misissuance	**2**
CRL Failures	**7**
DV Misissuance	**9**
EV Misissuance	**22**
Leaf Revocation Delays	**25**
OCSP Failures	**7**
OV Misissuance	**28**
Policy Failures	**24**
S/MIME Misissuance	**13**

Audit Delays and Findings (6): Findings from audits in 2023 and 2024 for CAs, such as Buypass, certSIGN, Microsec, SSL.com, and Telia and delayed audit statements for PKIoverheid's intermediate CAs.

CA Misissuance (2): Identrust had unintended creation of CA certificate and misuse of Policy Qualifiers in a CA.

CRL Failures (7): Failures related to CRLs, such as serving outdated CRLs, mismatched issuers, and non-conformance with TLS BRs by Asseco DS / Certum, CFCA, IdenTrust, Sectigo, e-commerce monitoring, and others.

DV Misissuance (9): Buypass, Google Trust Services, Microsec, NAVER Cloud Trust Services, SECOM, and others encountered problems with domain validation methods and subject attributes in issuing DV certificates.

EV Misissuance (22): ACCV, Actalis, Asseco-Certum, D-Trust, Digicert, Entrust, and others had incidents involving incorrect subject attributes, jurisdiction issues, and missing policy OIDs.

Leaf Revocation Delays (25): *Multiple CAs including Buypass, Certigna, certSIGN, CFCA, Chunghwa Telecom, Digicert, Entrust, and others had delays in revoking misissued certificates.*

OCSP Failures (7): Google Trust Services, HARICA, Microsoft PKI Services, VikingCloud, and others had issues with incorrect OCSP responses and/or post-software-upgrade anomalies.

OV Misissuance (28): ACCV, AGCE, Certigna, CFCA, Chunghwa Telecom, D-Trust, Disig, and others faced problems with basic constraints and incorrect information in OV certificates.

Policy Failures (24): Various policy implementation issues affected Entrust, CFCA, CommScope, D-Trust, Digicert, and others. These involved delayed responses to Certificate Problem Reports, incident reporting issues, errors or delays in updating CPSes, and failures in updating or implementing required certificate fields.

S/MIME Misissuance (13): DigiCert, GlobalSign, IdenTrust, Sectigo, SSL.com, SwissSign, and others had issues with S/MIME certificates not adhering to new requirements, including errors in subjectAlternativeNames, inconsistent issuance with S/MIME BRs, and incorrect document identification schemes.

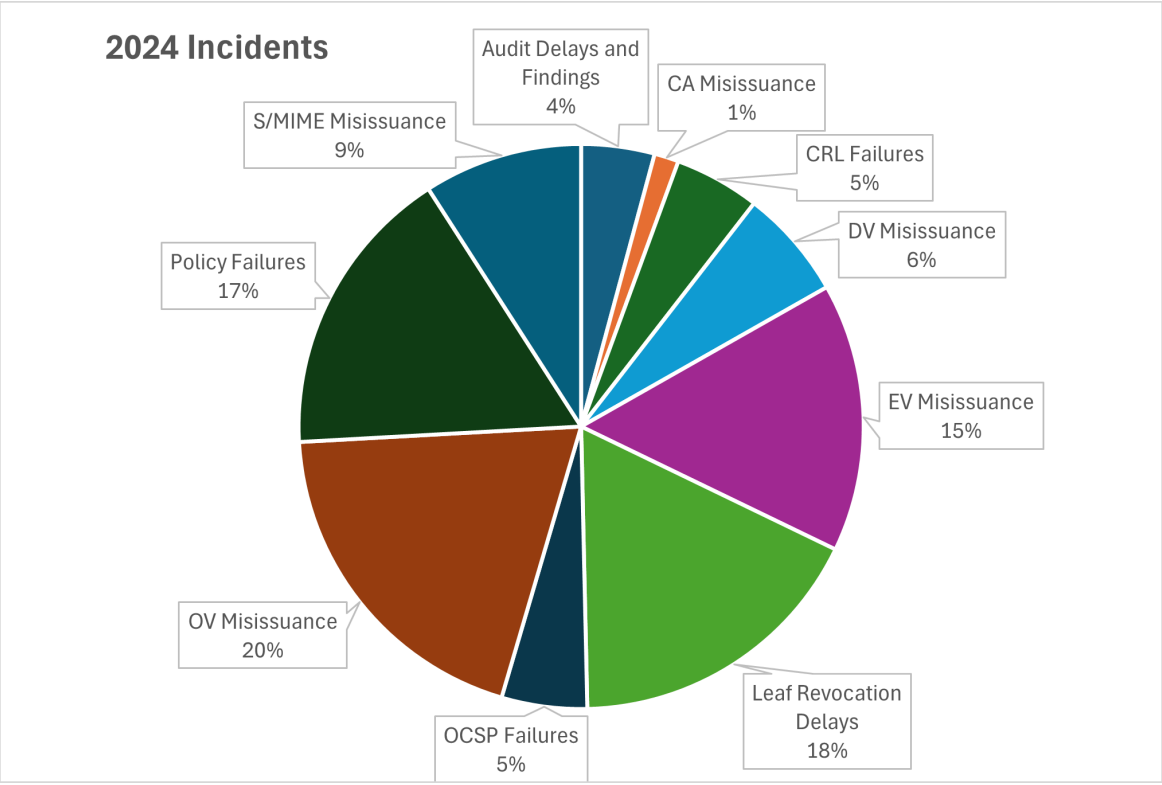

Chart based on 136 open incidents between January 1, 2024, and May 20, 2024.

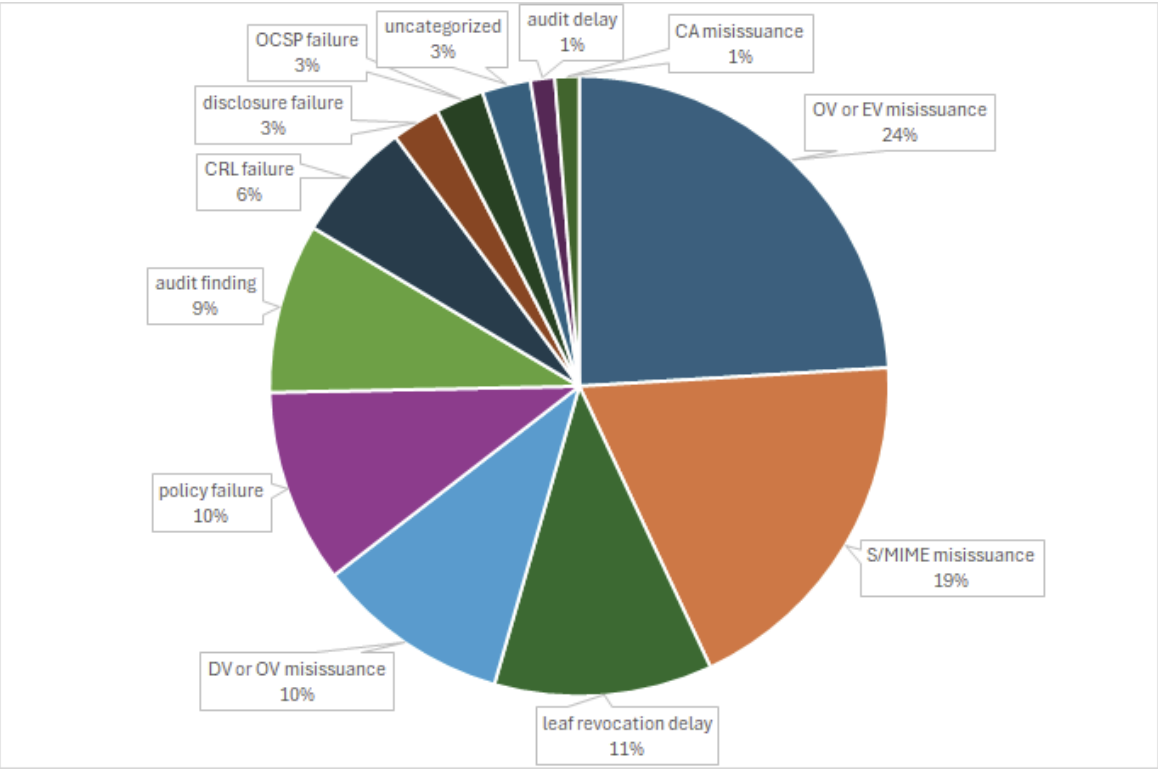

Chart based on 79 open incidents between October 1, 2023, and February 1, 2024

CA Inclusion Requests - https://wiki.mozilla.org/CA/Dashboard

Status	Count
Received - Initial Status	11
Information Verification	12
In Public Discussion (Taiwan CA & Cybertrust Japan)	2
TOTAL	**25**

Thunderbird

We have updated the process for creating a key pair and S/MIME certificate request (CSR). [Bug 1581796] The updates will be released in Thunderbird 128 (currently available in Daily/Nightly).
The S/MIME certificate request process includes these steps:

1. Create your public and secret key
2. Get a certificate using your public key from your Certificate Authority (CA)
3. Import the certificate into Thunderbird
4. Configure Thunderbird to use S/MIME security
5. Backup your certificate

Mozilla CA Certificate Program: **https://wiki.mozilla.org/CA**

Our Email Address: **certificates@mozilla.org**

Thanks!