B1. Spoofing the print service

An attacker impersonates the print service and thereby gains access to the documents the delivery manager sends

S of E1

Assets & consequences

- Documents are exposed to attacker – information disclosure
- Documents are not delivered to customers – reputation/billing

Comments
Possible because there is no authentication present

B2. Spoofing zoomit

An attacker impersonates zoomit and thereby gains access to the documents the delivery manager sends

S of E2

Assets & consequences

- Documents are exposed to attacker – information disclosure
- Documents are not delivered to customers – reputation/billing

Comments
Possible because there is no authentication present

B3. Spoofing the email provider

An attacker impersonates the email provider and thereby gains access to the documents the delivery manager sends

S of E3

Assets & consequences

- Documents are exposed to attacker – information disclosure
- Documents are not delivered to customers – reputation/billing

Comments
Possible because there is no authentication present

B4. Spoofing the PDS user to gain access to the PDS

An attacker impersonates the PDS user and thereby gains access to the documents of this specific user

S of E4

Assets & consequences

- User-specific documents are exposed to attacker – information disclosure

Comments
Possible through weak credential storage at client side

B5. Spoofing the PDS user by gaining access to one document URL

An attacker impersonates the PDS user as he gained access to an URL in transit and thereby gains access to this one specific document

S of E4

Assets & consequences

- Specific document is exposed to attacker – information disclosure

Comments

Possible because there is no encryption

B6. Spoofing the PDS user by guessing document URL

An attacker impersonates the PDS user by guessing the document URL of the user and thereby gains access to this one specific document

S of E4

Assets & consequences

- Specific document is exposed to attacker – information disclosure
- Possibly all documents are exposed (depending on how easy to guess url is)

Comments

Possible because of predictable credentials – easy to guess urls

B7. Spoofing the PDS user by false user registration

An attacker impersonates a PDS user by pretending to be this person at user registration and thereby gains access to **the user's** documents

S of E4

Assets & consequences

- One user's documents are exposed to attacker – information disclosure

Comments

Possible because there is no identity verification

B8. Repudiation by print service

The print service denies having received documents from the delivery manager

R of E1

Assets & consequences

- Batch of documents is not delivered / SLA agreement

B9. Repudiation by zoomit

Zoomit denies having received documents from the delivery manager

R of E2

Assets & consequences

- Batch of documents is not delivered / SLA agreement

B10. Repudiation by email provider

The email provider denies having received documents from the delivery manager

R of E3

Assets & consequences

- Batch of documents is not delivered / SLA agreement

B11. Repudiation of document request by PDS user

The PDS user denies having requested documents from the PDS

R of E4

Assets & consequences

- Reputation/billing

Comments

PDS user claims to be spoofed

B12. Repudiation of document retrieval by PDS user

The PDS user denies having retrieved a document URL

R of E4

Assets & consequences

- Reputation/billing

Comments

PDS user claims URL was guessed/intercepted

B13. Spoofing the delivery manager

The attacker pretends to be the delivery manager and gains access to delivery status messages

S of P2

Assets & consequences

- Disclosure of delivery status and ID
- Missing delivery notifications

Comments

Attacker substitutes delivery manager link (e.g. phishing)

B14. Spoofing the PDS

The attacker pretends to be the PDS and gains access to user information (i.e. credentials)

S of P3

Assets & consequences

- Disclosure of user credentials, document URLs, user registration information

Comments

Attacker substitutes delivery manager link (e.g. phishing)

B15. Tampering with the generated docs archive

The attacker tampers with the delivery status and IDs of the generated docs archive

T of DS1

Assets & consequences

- Integrity of generated documents archive

Comments

There is no authorization

B16. Tampering with the generated docs archive

The attacker tampers with the delivery status and IDs of the generated docs archive

T of DS3

Assets & consequences

- Integrity of user data (credentials/email)

Comments

There is no authorization

B17. Information disclosure of PDS docs

The attacker gains access to the documents in the PDS datastore

I of DS2

Assets & consequences

- Disclosure of PDS docs

Comments

There is no authentication/ attacker can spoof user

B18. Repudiation of zoomit delivery status

The customer claims not to have received the zoomit document

R of DS1

Assets & consequences

- Zoomit delivery status

Comments

No trusted process to log delivery/ insufficient metadata/ no attestation

B19. Repudiation of email delivery status

The customer claims not to have received the emailed document

R of DS1

Assets & consequences

- Email delivery status

Comments

No trusted process to log delivery/ insufficient metadata/ no attestation

B20. Tampering with outgoing email flow

The attacker changes the PDF or URL sent to the email provider

T of DF4

Assets & consequences

- Document content integrity

Comments

Attacker changes email content (e.g. URL, account/bank number,…). Threat is possible because flow is not encrypted.

B21. Tampering with email notification flow

The attacker changes the delivery message sent by the email provider

T of DF5

Assets & consequences

- Delivery status integrity

Comments

Threat is possible because flow is not encrypted.

B22. Information disclosure of outgoing email flow

The attacker gains access to the PDF or URL sent to the email provider

I of DF4

Assets & consequences

- Document content disclosure
- URL disclosure can lead to spoofing threat B5

Comments

Threat is possible because flow is not encrypted.

B23. Information disclosure of email notification flow

The attacker gains access to the delivery message sent by the email provider

I of DF5

Assets & consequences

- Delivery status disclosure

Comments

Threat is possible because flow is not encrypted.

B24. Spoofing the delivery manager to send fake documents to the print service

The attacker pretends to be the delivery manager and sends fake documents to the print service. The print service then bills e-docs for these fake documents.

S->T of P2

Assets & consequences

- Availability (DoS)/Reputation/billing

B25. Spoofing the delivery manager to send fake documents to the email provider

The attacker pretends to be the delivery manager and sends fake documents to the email provider. The email provider then bills e-docs for these fake documents.

S->T of P2

Assets & consequences

- Availability (DoS)/Reputation/billing

B26. Spoofing the delivery manager to send fake documents to zoomit

The attacker pretends to be the delivery manager and sends fake documents to zoomit. Zoomit then bills e-docs for these fake documents.

S->T of P2

Assets & consequences

- Availability (DoS)/Reputation/billing

B27. Spoofing zoomit to send fake delivery messages

The attacker pretends to be zoomit and sends fake delivery messages to the delivery manager.

S->T of E2

Assets & consequences

- fake delivery status

B28. Spoofing email provider to send fake delivery messages

The attacker pretends to be the email provider and sends fake delivery messages to the delivery manager.

S->T of E3

Assets & consequences

- fake delivery status