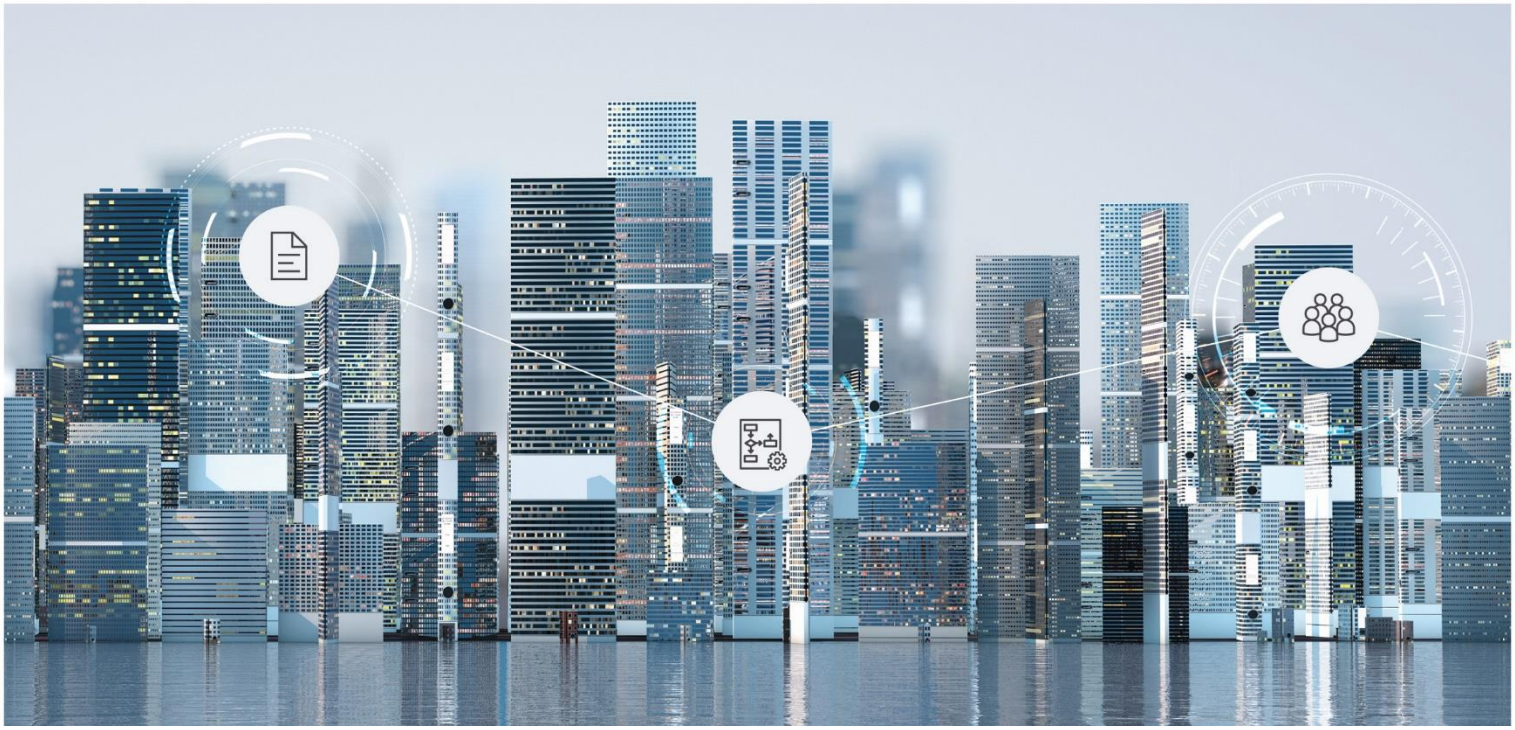
Fabasoft®



Security Vulnerabilities

Fabasoft Folio

Aus Gründen der einfacheren Lesbarkeit wird auf die geschlechtsspezifische Differenzierung, z. B. Benutzer/-innen, verzichtet. Entsprechende Begriffe gelten im Sinne der Gleichbehandlung grundsätzlich für beide Geschlechter.

Inhalt

1 Vulnerabilities 2024

1.1 Workflow XSS security vulnerability (eGov16804)

First published: 11 September 2024 (restricted disclosure)

Last update: 11 October 2024

ID: eGov16804

Affected Components: Fabasoft eGov-Suite versions from 2021 up to 2024

Severity: CVSS:4.0/AV:A/AC:L/AT:N/PR:L/UI:A/VC:H/VI:H/VA:H/SC:L/SI:L/SA:N, Base Score: 7.0 / HIGH

Status: Final

CVEs: -

1.1.1 Summary

A potential cross-site scripting (XSS) issue has been identified concerning the workflow feature.

To exploit this vulnerability a potential attacker must be authenticated as a valid user.

1.1.2 Impact

After successful exploitation of this vulnerability, arbitrary JavaScript code may be executed in the user's web browser.

1.1.3 Remediation

The vulnerability can be remediated by installing a hotfix provided by Fabasoft.

1.1.3.1 Hotfix information

Fabasoft provides hotfixes for the following Fabasoft eGov-Suite versions:

- Fabasoft eGov-Suite 2021 Update Rollup 3 (included with 21.1.3.089.152)
- Fabasoft eGov-Suite 2022 Update Rollup 2 (included with 22.0.2.079.165)
- Fabasoft eGov-Suite 2022 Update Rollup 3 (included with 22.0.3.075.044)
- Fabasoft eGov-Suite 2023 September Release (included with 23.9.0.280.027)
- Fabasoft eGov-Suite 2023 Update Rollup 1 (included with 23.0.1.088.036)
- Fabasoft eGov-Suite 2023 Update Rollup 2 (included with 23.0.2.057.084)
- Fabasoft eGov-Suite 2023 Update Rollup 3 (included with 23.0.3.053.135)
- Fabasoft eGov-Suite 2024 April Release (included with 24.4.0.355.032)
- Fabasoft eGov-Suite 2024 June Release (included with 24.6.0.301.024)
- Fabasoft eGov-Suite 2024 Update Rollup 1 (included with 24.0.1.043.038)
- Fabasoft eGov-Suite 2024 Update Rollup 2 (included with 24.0.2.020.092)

The fix for this vulnerability is already included with the following and newer versions:

- Fabasoft eGov-Suite 2024 September Release
- Fabasoft eGov-Suite 2024 Update Rollup 3

1.2 Document redaction XSS security vulnerability (eGov16750)

First published: 05 August 2024 (restricted disclosure)

Last update: 05 September 2024

ID: eGov16750

Affected Components: Fabasoft eGov-Suite versions from 2022 up to 2024 with activated browser annotation feature

Severity: CVSS:4.0/AV:A/AC:L/AT:N/PR:L/UI:A/VC:H/VI:H/VA:H/SC:L/SI:L/SA:N, Base Score: 7.0 / High

Status: Final

CVEs: -

1.2.1 Summary

A potential cross-site scripting (XSS) issue has been identified concerning the document redaction feature.

The vulnerability can only be exploited if "Browser" is selected as "Annotation Software" in the Fabasoft eGov-Suite. In addition, a potential attacker must be authenticated as a valid user.

1.2.2 Impact

After successful exploitation of this vulnerability, arbitrary JavaScript code may be executed in the user's web browser.

1.2.3 Remediation

The vulnerability can be remediated by installing a hotfix provided by Fabasoft.

1.2.3.1 Hotfix information

Fabasoft provides hotfixes for the following Fabasoft eGov-Suite versions:

- Fabasoft eGov-Suite 2022 Update Rollup 2 (included with 22.0.2.75.164)
- Fabasoft eGov-Suite 2022 Update Rollup 3 (included with 22.0.3.70.41)
- Fabasoft eGov-Suite 2023 September Release (included with 23.9.0.280.26)
- Fabasoft eGov-Suite 2023 Update Rollup 1 (included with 23.0.1.81.35)
- Fabasoft eGov-Suite 2023 Update Rollup 2 (included with 23.0.2.50.83)
- Fabasoft eGov-Suite 2023 Update Rollup 3 (included with 23.0.3.42.127)
- Fabasoft eGov-Suite 2024 (included with 24.0.0.224.25)
- Fabasoft eGov-Suite 2024 April Release (included with 24.4.0.355.31)
- Fabasoft eGov-Suite 2024 June Release (included with 24.6.0.301.21)
- Fabasoft eGov-Suite 2024 Update Rollup 1 (included with 24.0.1.38.31)

The fix for this vulnerability is already included with the following and newer versions:

- Fabasoft eGov-Suite 2024 Update Rollup 2
- Fabasoft eGov-Suite 2024 September Release

1.3 Arbitrary JavaScript execution in PDF.js (eGov16581, MINDBREEZE31126)

First published: 10 June 2024 (restricted disclosure)

Last update: 11 July 2024

ID: eGov16581, MINDBREEZE31126

Affected Components:

- Fabasoft eGov-Suite versions up to 2024 Update Rollup 1
- Fabasoft Mindbreeze Enterprise versions up to 24.3.0.268

Severity: CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:L/SI:L/SA:N, Base Score: 8.5 / High

Status: Final

CVEs: CVE-2024-4367

1.3.1 Summary

A type check was missing when handling fonts in the third-party library PDF.js, which would allow arbitrary JavaScript execution in the PDF.js context.

1.3.2 Impact

After successful exploitation of this vulnerability, arbitrary JavaScript code may be executed in the user's web browser.

1.3.3 Remediation

1.3.3.1 Fabasoft eGov-Suite

The vulnerability affecting the Fabasoft eGov-Suite can be remediated by installing a hotfix provided by Fabasoft.

1.3.3.1.1 Hotfix information

Fabasoft provides hotfixes for the following Fabasoft eGov-Suite versions:

- Fabasoft eGov-Suite 2020 Update Rollup 5 (included with 20.1.5.85.51)
- Fabasoft eGov-Suite 2021 Update Rollup 3 (included with 21.1.3.86.150)
- Fabasoft eGov-Suite 2022 Update Rollup 2 (included with 22.0.2.75.163)
- Fabasoft eGov-Suite 2022 Update Rollup 3 (included with 22.0.3.70.40)
- Fabasoft eGov-Suite 2023 September Release (included with 23.9.0.273.23)
- Fabasoft eGov-Suite 2023 Update Rollup 1 (included with 23.0.1.81.34)
- Fabasoft eGov-Suite 2023 Update Rollup 2 (included with 23.0.2.50.82)
- Fabasoft eGov-Suite 2023 Update Rollup 3 (included with 23.0.3.36.123)
- Fabasoft eGov-Suite 2024 (included with 24.0.0.214.23)
- Fabasoft eGov-Suite 2024 April Release (included with 24.4.0.355.22)
- Fabasoft eGov-Suite 2024 Update Rollup 1 (included with 24.0.1.25.28)

The fix for this vulnerability is already included with the following and newer versions:

- Fabasoft eGov-Suite 2024 Update Rollup 2
- Fabasoft eGov-Suite 2024 June Release

1.3.3.2 Fabasoft Mindbreeze Enterprise

The vulnerability affecting Fabasoft Mindbreeze Enterprise can be remediated by installing Fabasoft Mindbreeze Enterprise version 24.3.1.271 or newer.

For older Fabasoft Mindbreeze Enterprise versions, a remediation by editing a file on the Fabasoft Mindbreeze Enterprise server is available:

- Open the following file for editing:

    - Linux: `/opt/mindbreeze/bin/webapps/client-service/ROOT/apps/scripts/pdfjs-dist/build/pdf.js`
    - Windows: `C:\Program Files\Mindbreeze\Enterprise Search\Server\webapps\client-service\ROOT\apps\scripts\pdfjs-dist\build\pdf.js`
- Search for line `return globalSettings ? globalSettings.isEvalSupported : true;`
- Replace the line with `return false;`
- The cache will be removed within 1 hour and the client will use the patched file to open PDF.

If you need further assistance, please open a Fabasoft Support Ticket.

2 Vulnerabilities 2023

2.1 Mindbreeze security update for Basic Authentication (MINDBREEZE29751)

First published: 18 December 2023

Last update: 20 December 2023

ID: MINDBREEZE29751

Affected Components:

- Fabasoft Mindbreeze Enterprise (Linux) with active Kerberos client authentication
- Mindbreeze InSpire G7 with active Kerberos client authentication

Severity: Critical

Status: Final

CVEs: -

Original publication: https://inspire.mindbreeze.com/support/vulnerabilities/security-update-to-disable-keytab-in-jaas-login-configuration-for-basic-authentication-mindbreeze29751

2.1.1 Summary

When using Kerberos authentication for Mindbreeze under Linux, an attacker can in particular circumstances impersonate a user.

This vulnerability only can occur if all of the following circumstances are met:

- Mindbreeze InSpire or Fabasoft Mindbreeze Enterprise is running under Linux
- Kerberos authentication is configured

Fabasoft Mindbreeze Enterprise installed on Microsoft Windows is not affected.

2.1.2 Impact

After successful exploitation of this vulnerability, the attacker assimilates the same level of access as the user normally has, gaining access to index search results of this user.

2.1.3 Remediation

The vulnerability can be remediated by installing the hotfix listed below.

For older Fabasoft Mindbreeze Enterprise versions, a remediation by changing configuration on the Mindbreeze server is available:

- Open the Java Kerberos configuration for editing: `/etc/mindbreeze/java-krb5.conf`

- Search for the Login Configuration `com.mindbreeze.auth.basic`
- Change the `useKeyTab` parameter to `false`:
  - `useKeyTab = false`
- Remove the following parameter from the section:
  - `keyTab="${keytabpath}"`

```
com.mindbreeze.auth.basic {
    com.sun.security.auth.module.Krb5LoginModule required
    useKeyTab=false
    useTicketCache=false
    forwardable=true;
};
```

If you need further assistance, please open a Fabasoft Support Ticket.

2.1.4 Hotfix information

Mindbreeze provides a hotfix for the following Fabasoft Mindbreeze Enterprise version:

- Fabasoft Mindbreeze Enterprise 23.6 (23.6.3.336)

Higher versions and build numbers of Fabasoft Mindbreeze Enterprise implicitly include the hotfix.

2.2 Object list XSS security vulnerability (PDO07741)

First published: 20 July 2023 (restricted disclosure)

Last update: 29 August 2023

ID: PDO07741

Affected Components:

- Fabasoft Folio and Fabasoft eGov-Suite 2023 Update Rollup 1
- Fabasoft eGov-Suite 2023 April and June Release

Severity: CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N Base Score: 7.3

Status: Closed

CVEs: -

2.2.1 Summary

During thorough testing of Fabasoft Folio/eGov-Suite a potential cross-site scripting issue has been identified concerning grouped object lists in detail view.

Only Fabasoft Folio/eGov-Suite 2023 Update Rollup 1 and Feature Track are affected, versions below Fabasoft Folio/eGov-Suite 2023 Update Rollup 1 are not affected.

2.2.2 Impact

While using a grouped object lists in detail view a potential cross-site scripting (XSS) vulnerability has been identified which could be exploited to inject malicious script code into the installation of Fabasoft Folio/eGov-Suite.

2.2.3 Remediation

The vulnerability can be remediated by installing a hotfix provided by Fabasoft.

2.2.4 Hotfix information

Fabasoft provides hotfixes for the following Fabasoft Folio/eGov-Suite versions:

- Fabasoft Folio/eGov-Suite 2023 Update Rollup 1 (included with 23.0.1.65)
- Fabasoft eGov-Suite 2023 April Release (included with 23.4.0.241)
- Fabasoft eGov-Suite 2023 June Release (included with 23.6.0.324)

The fix for this vulnerability is already included with the following and newer versions:

- Fabasoft Folio/eGov-Suite 2023 Update Rollup 2
- Fabasoft eGov-Suite 2023 September Release

2.3 Ghostscript pipe security vulnerability (CVE-2023-36664)

First published: 18 July 2023 (restricted disclosure)

Last update: 29 August 2023 (gs)

ID: CVE-2023-36664

Affected Components:

- Fabasoft Folio and eGov-Suite installations that use Artifex Ghostscript as a conversion tool

Severity: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H Base Score: 7.8

Status: Open

CVEs: CVE-2023-36664

2.3.1 Summary

A security vulnerability has been identified and classified as CVE-2023-36664 that allows the exploitation of Artifex Ghostscript with a specifically crafted PDF document.

2.3.2 Impact

On installations of Fabasoft Folio/eGov-Suite that use Artifex Ghostscript as a conversion tool, it is possible that an attacker could exploit this vulnerability in Ghostscript, it is therefore recommended to perform steps to mitigate this scenario.

2.3.3 Remediation

Based on internal testing, installations of Fabasoft Folio/eGov-Suite 2022 Update Rollup 1 (22.0.1) and newer can successfully perform conversion operations using a version of Artifex Ghostscript that includes a fix for CVE-2023-36664.

Older versions of Fabasoft Folio/eGov-Suite using newer versions of Artifex Ghostscript abort conversion operations with an error.

If an affected system does not support a version of Ghostscript that includes a fix for CVE-2023-36664, it is possible to remove or disable Artifex Ghostscript on the conversion servers, but this operation will also affect or disable some features including the following:

- Import of files with the Fabasoft Folio Printer Ports.
- Redaction of documents in Fabasoft eGov-Suite. (Schwärzung)
- Indirect PDF conversion of documents via printing to Postscript.

2.3.4 Hotfix information

The following versions of Fabasoft Folio and the Fabasoft eGov-Suite can use a fixed version of Artifex Ghostscript as a conversion tool:

- Fabasoft Folio/eGov-Suite 2022 Update Rollup 1
- Fabasoft Folio/eGov-Suite 2022 Update Rollup 2
- Fabasoft Folio/eGov-Suite 2022 Update Rollup 3
- Fabasoft eGov-Suite 2022 September Release
- Fabasoft Folio/eGov-Suite 2023
- Fabasoft Folio/eGov-Suite 2023 Update Rollup 1
- Fabasoft Folio/eGov-Suite 2023 April Release
- Fabasoft Folio/eGov-Suite 2023 June Release

The following versions of Fabasoft Folio and the Fabasoft eGov-Suite can use a fixed version of Artifex Ghostscript after the installation of a relevant hotfix:

- Fabasoft Folio/eGov-Suite 2016 Update Rollup 7 (included with 16.0.11.86)
- Fabasoft Folio/eGov-Suite 2017 R1 (included with 17.4.0.73)
- Fabasoft Folio/eGov-Suite 2020 Update Rollup 5 (included with 20.1.5.81)
- Fabasoft Folio/eGov-Suite 2021 Update Rollup 3 (included with 21.1.3.82)
- Fabasoft Folio/eGov-Suite 2022 (included with 22.0.0.284)

Other versions are currently being evaluated, future updates to this article may extend the list of compatible versions.

2.4 Import path security vulnerability (eGov15419)

First published: 29 June 2023 (restricted disclosure)

Last update: 29 July 2023

ID: eGov15419

Affected Components:

- Fabasoft eGov-Suite versions up to 2023 April Release

Severity: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H Base Score: 8.8

Status: Closed

CVEs: -

2.4.1 Summary

In a Fabasoft eGov-Suite import feature, a normal user is able to configure any import path without restrictions, leading to a possible security issue when restricted operating system files get imported.

Only Fabasoft eGov-Suite systems are affected as this import feature is only available in Fabasoft eGov-Suite.

Fabasoft Folio is not affected by the vulnerability.

2.4.2 Impact

After the import, the user will have full access to the imported files. That files usually would be restricted in the original file system folder of the web server.

Due to this import the imported files may be deleted at the original location. This could lead to configuration failures or data loss on the affected webserver.

2.4.3 Remediation

The vulnerability can be remediated by installing a hotfix provided by Fabasoft.

2.4.4 Hotfix information

Fabasoft provides hotfixes for the following Fabasoft Folio/eGov-Suite versions:

- Fabasoft eGov-Suite 2019 Update Rollup 3 (included with 19.2.3.141.53)
- Fabasoft eGov-Suite 2020 Update Rollup 5 (included with 20.1.5.78.46)
- Fabasoft eGov-Suite 2021 Update Rollup 3 (included with 21.1.3.78.146)
- Fabasoft eGov-Suite 2022 Update Rollup 1 (included with 22.0.1.56.32)
- Fabasoft eGov-Suite 2022 Update Rollup 2 (included with 22.0.2.65.158)
- Fabasoft eGov-Suite 2022 Update Rollup 3 (included with 22.0.3.49.31)
- Fabasoft eGov-Suite 2022 June Release (included with 22.6.0.363.36)
- Fabasoft eGov-Suite 2022 September Release (included with 22.9.0.353.22)
- Fabasoft eGov-Suite 2023 (included with 23.0.0.227.62)
- Fabasoft eGov-Suite 2023 Update Rollup 1 (included with 23.0.1.48.27)
- Fabasoft eGov-Suite 2023 April Release (included with 23.4.0.229.7)

The vulernability is directly fixed within the releases of

- Fabasoft eGov-Suite 2023 Update Rollup 2 (and later Update Rollups and major releases)
- Fabasoft eGov-Suite 2023 June Release (and later Feature releases)

2.5 Client AutoUpdate Harmful Code Installation Vulnerability (PDO06614)

First published: 8 May 2023 (restricted disclosure)

Last update: 4 July 2023

ID: PDO06614

Affected Components: Fabasoft Folio / Fabasoft eGov-Suite 2021 UR3, Fabasoft Folio / Fabasoft eGov-Suite 2022 (incl. all URs), Fabasoft Folio/eGov-Suite 2023 (incl. UR1), Fabasoft Cloud

Severity: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H Total Score: 8,8 HIGH

Status: Final

CVEs: -

2.5.1 Summary

A privilege escalation is possible by an intruder on a Microsoft Windows client using the Fabasoft Folio/Cloud Client AutoUpdate-Service (installed with the Fabasoft Folio Client from Fabasoft Folio/eGov-Suite 2021 or the Fabasoft Cloud Enterprise Client).

Affected Fabasoft Folio / Fabasoft eGov-Suite versions:

- Fabasoft Folio / eGov-Suite 2021 Update Rollup 3
- Fabasoft Folio / eGov-Suite 2022 (up to Update Rollup 3 and Feature Track)
- Fabasoft Folio / eGov-Suite 2023 (up to Update Rollup 1)
- Fabasoft Cloud

Versions below Fabasoft Folio / eGov-Suite 2021 Update Rollup 3 are not affected.

Linux and Apple macOS clients are not affected.

2.5.2 Impact

In the case the vulnerability could be exploited, malicious software can be installed and executed on the client PC.

2.5.3 Remediation

Fabasoft provides a hotfix for the Fabasoft Folio Client for the affected Fabasoft Folio / eGov-Suite versions. Please install/roll-out this hotfix immediately. If it is not possible to immediately update the Fabasoft Folio Client, see the possible workaround to disable the Fabasoft Folio Client Update Service below.

2.5.3.1 Fabasoft Cloud

The current download of the Fabasoft Cloud Client from the Fabasoft Cloud already includes the hotfixed version of the Fabasoft Cloud Client.

If the Fabasoft Cloud Client is already installed, the update to the hotfixed version is triggered automatically.

2.5.3.2 Hotfix information Fabasoft Folio / Fabasoft eGov-Suite

Fabasoft provides the hotfixed Fabasoft Folio Client for the affected versions in the following teamroom:

https://at.cloud.fabasoft.com/folio/public/3rz6bra2xcba40s6gt5fishghl

Only the Fabasoft Folio Client on Windows PCs needs to be updated. There is no need to update the Fabasoft Folio / eGov-Suite domain.

The following Fabasoft Folio Client build numbers include the correction:

- 23.4.0.66 and above
- 23.0.1.23 and above
- 22.9.0.75 and above
- 22.0.3.88 and above
- 21.1.3.204 and above

2.5.3.3 Workaround: Disable Fabasoft Folio Client Update Service

The affected part of the Fabasoft Folio Client is the Fabasoft Folio Client Update Service, that is installed during the Fabasoft Folio Client installation.

This service is listed under Windows Services as

- "Fabasoft Folio Client 2023 Update Service", service name is "folioupdatepm23".
- "Fabasoft Folio Client 2022 Update Service", service name is "folioupdatepm22".
- "Fabasoft Folio Client 2021 Update Service", service name is "folioupdatepm21".

Set the service startup type to "Disabled" via Group Policy. By disabling these services, the security vulnerability cannot be exploited.

The Fabasoft Folio Client Update Service may not be installed or enabled on your clients, therefore the vulnerability cannot be exploited. Nevertheless we recommend to update the Fabasoft Folio Client.

2.6 LDAP authentication vulnerability

First published: 25 April 2023 (restricted disclosure)

Last update: 30 May 2023

ID: PDO06544

Affected Components:

- All Fabasoft Folio/eGov-Suite versions up to 2023 UR1

Severity: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N, Base Score: 9.1

Status: Closed

CVEs: -

2.6.1 Summary

When using the integrated LDAP authentication, an attacker can in particular circumstances impersonate a user.

Only systems using the integrated LDAP authentication feature of Fabasoft Folio are affected. It does not affect LDAP authentication via an external SAML identity provider.

The CVSS severity is reduced if LDAP authentication is only available over a local network: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N, Base Score: 8.1

2.6.2 Impact

After successful exploitation of this vulnerability, the attacker assumes all privileges of the compromised user account, with the same level of access to all objects and actions as the user normally has.

2.6.3 Remediation

The vulnerability can be remediated by installing one of the hotfixes listed below.

2.6.4 Hotfix information

Fabasoft provides hotfixes for the following Fabasoft Folio/eGov-Suite versions:

- Fabasoft Folio/eGov-Suite 2016 Update Rollup 7 (included with 16.0.11.85)
- Fabasoft Folio/eGov-Suite 2017 R1 (included with 17.4.0.71)
- Fabasoft Folio/eGov-Suite 2019 Update Rollup 3 (included with 19.2.3.141)
- Fabasoft Folio/eGov-Suite 2020 Update Rollup 5 (included with 20.1.5.78)
- Fabasoft Folio/eGov-Suite 2021 Update Rollup 3 (included with 21.1.3.77)
- Fabasoft Folio/eGov-Suite 2022 (included with 22.0.0.283)
- Fabasoft Folio/eGov-Suite 2022 Update Rollup 1 (included with 22.0.1.55)
- Fabasoft Folio/eGov-Suite 2022 Update Rollup 2 (included with 22.0.2.63)
- Fabasoft Folio/eGov-Suite 2022 Update Rollup 3 (included with 22.0.3.48)
- Fabasoft Folio/eGov-Suite 2022 September Release (included with 22.9.0.352)

- Fabasoft Folio/eGov-Suite 2023 (included with 23.0.0.226)
- Fabasoft Folio/eGov-Suite 2023 Update Rollup 1 (included with 23.0.1.18)
- Fabasoft Folio/eGov-Suite 2023 April Release (included with 23.4.0.228)

2.7 HTML Injection and Cross-Site Scripting in Time Travel Feature (eGov14917)

First published: 23 January 2023

Last update: 25 January 2023

ID: eGov14917

Affected Components:

- Fabasoft eGov-Suite 2019
- Fabasoft eGov-Suite 2020
- Fabasoft eGov-Suite 2021
- Fabasoft eGov-Suite 2022

Severity: CVSS:3.1/AV:A/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:N, Base Score: 8.1

Status: Final

CVEs: -

2.7.1 Summary

An input field of the Time Travel feature in the Fabasoft eGov-Suite is vulnerable to HTML injection and stored cross-site scripting.

To exploit this vulnerability an attacker has to be authenticated as a valid user.

The vulnerability only concerns Fabasoft eGov-Suite, but not Fabasoft Folio.

2.7.2 Impact

An attacker could insert HTML or JavaScript code into the affected Time Travel input field of an object (e.g. document). If another user has access to this object and opens the Time Travel feature, the inserted HTML or JavaScript code may be executed in the user's web browser.

2.7.3 Remediation

The vulnerability can be remediated by installing one of the hotfixes listed below.

2.7.4 Hotfix information

Fabasoft provides hotfixes for the following Fabasoft eGov-Suite versions:

- Fabasoft eGov-Suite 2022 September Release
- Fabasoft eGov-Suite 2022 June Release
- Fabasoft eGov-Suite 2022 Update Rollup 2
- Fabasoft eGov-Suite 2021 Update Rollup 3
- Fabasoft eGov-Suite 2020 Update Rollup 5

The fix **is already included** starting with the following Fabasoft eGov-Suite build numbers:

- Fabasoft eGov-Suite 2023
- Fabasoft eGov-Suite 2022 Update Rollup 3

- Fabasoft eGov-Suite 2022 September Release from build 22.9.0.344.19
- Fabasoft eGov-Suite 2022 June Release from 22.6.0.363.035
- Fabasoft eGov-Suite 2022 Update Rollup 2 from 22.0.2.56.149
- Fabasoft eGov-Suite 2021 Update Rollup 3 from 21.1.3.63.142
- Fabasoft eGov-Suite 2020 Update Rollup 5 from 20.1.5.75.44
- and any later major releases and Update Rollups.

3 Vulnerabilities 2022

3.1 Text4Shell CVE-2022-42889 information

First published: 21 October 2022

Last update: 27 October 2022

ID: PDO03176

3.1.1 Summary

Apache Commons Text library filed a security vulnerability CVE-2022-42889 that allows arbitrary code execution or contact with remote servers.

Fabasoft Folio and Fabasoft Business Process Cloud include the library, but **do not use any function that is affected by the security vulnerability**.

Nevertheless Fabasoft will update the library in its products as precaution.

3.1.2 Impact

No Fabasoft products are impacted by the Text4Shell vulnerability.

3.1.3 Remediation

Although no Fabasoft product is using a vulnerable function of the library, Fabasoft will update the Apache Commons Text library in its products.

3.1.3.1 Fabasoft Business Process Cloud

The Fabasoft Business Process Cloud will be updated on 26th October 2022 with the latest fixed Apache Commons Text library.

3.1.3.2 Fabasoft Folio / Fabasoft eGov-Suite

A preventative hotfix with the updated Apache Commons Text library will be released. See the list of versions below.

3.1.4 Hotfix information

The Apache Commons Text library is part of Fabasoft Folio / Fabasoft eGov-Suite, but no Fabasoft product is affected by the vulnerable functions of the library.

For precaution, Fabasoft provides hotfixes for the following versions:

- Fabasoft Folio / Fabasoft eGov-Suite 2022 September Release (from 22.9.0.326)
- Fabasoft Folio / Fabasoft eGov-Suite 2022 June Release (from 22.6.0.365)

- Fabasoft Folio / Fabasoft eGov-Suite 2022 April Release (from 22.4.0.363)
- Fabasoft Folio / Fabasoft eGov-Suite 2022 Update Rollup 2 (from 22.0.2.38)
- Fabasoft Folio / Fabasoft eGov-Suite 2022 Update Rollup 1 (from 22.0.1.49)
- Fabasoft Folio / Fabasoft eGov-Suite 2022 (from 22.0.0.278)

Versions before Fabasoft Folio / Fabasoft eGov-Suite 2022 do not include the Apache Commons Text library.

3.2 Cross Site Scripting due to Object Pointers in Detail View (PDO01731)

First published: 15 July 2022

Last update: 19 July 2022

ID: PDO01731

Affected Components: Fabasoft Cloud, Fabasoft Folio Version 2022 June Release from build 260 to build 303 (22.6.0.260 - 22.6.0.303)

Severity: CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N, Basic Score: 7.3

Status: Final

CVEs: -

3.2.1 Summary

Malicious contents can be injected on the web browser client in a detail view.

3.2.2 Impact

An attacker may create an object with the malicious content in the name. If the object is shown in the detail view, code may be executed in the current usersâ€™ context in the browser.

3.2.3 Remediation

The cross site scripting vulnerability is fixed.

3.2.3.1 Fabasoft Cloud

A hotfix was applied in the Fabasoft Cloud at 15. July 2022.

3.2.3.2 Fabasoft Folio

A hotfix is provided for Fabasoft Folio Version 2022 June Release. It is recommended to install this hotfix.

3.2.4 Hotfix Information

Fixed with following versions Fabasoft Folio:

Fabasoft Folio Version 2022 June Release (Version 22.6.0. 304)

3.3 Client AutoUpdate Harmful Code Installation Vulnerability (FSC33251)

First published: 21 April 2022

Last update: 25 April 2022

ID: FSC33251

Affected Components: Fabasoft Folio / Fabasoft eGov-Suite 2021 UR3, Fabasoft Folio / Fabasoft eGov-Suite 2022, Fabasoft Business Process Cloud

Severity: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H Total Score: 8,8 HIGH

Status: Final

CVEs: -

3.3.1 Summary

A privilege escalation is possible by an intruder on a Microsoft Windows client using the Fabasoft Folio/Cloud Client AutoUpdate-Service (installed with the Fabasoft Folio Client from Fabasoft Folio/eGov-Suite 2021 or the Fabasoft Cloud Enterprise Client).

Affected Fabasoft Folio / Fabasoft eGov-Suite versions:

- Fabasoft Folio / eGov-Suite 2021 Update Rollup 3
- Fabasoft Folio / eGov-Suite 2022
- Fabasoft Business Process Cloud

Versions below Fabasoft Folio / eGov-Suite 2021 Update Rollup 3 are not affected.

Linux and Apple macOS clients are not affected.

3.3.2 Impact

In the case the vulnerability could be exploited, malicious software can be installed and executed on the client PC.

3.3.3 Remediation

Fabasoft provides a hotfix for the Fabasoft Folio Client for the affected Fabasoft Folio / eGov-Suite versions. Please install/roll-out this hotfix immediately. If it is not possible to immediately update the Fabasoft Folio Client, see the possible workaround to disable the Fabasoft Folio Client Update Service below.

3.3.3.1 Fabasoft Business Process Cloud

The current download of the Fabasoft Cloud Client from the Fabasoft Business Process Cloud already includes the hotfixed version of the Fabasoft Cloud Client.

If the Fabasoft Cloud Client is already installed, the update to the hotfixed version is triggered automatically.

3.3.3.2 Hotfix information Fabaosoft Folio / Fabasoft eGov-Suite

Fabasoft provides the hotfixed Fabasoft Folio Client for the affected versions in the following teamroom:

https://at.cloud.fabasoft.com/folio/public/0vmm5s2yvqt5p0pryhjkscvi57

Only the Fabasoft Folio Client on Windows PCs needs to be updated. There is no need to update the Fabasoft Folio / eGov-Suite domain.

The following Fabasoft Folio Client build numbers include the correction:

- 22.4.0.45 and above

- 22.2.0.32 and above
- 22.0.0.80 and above
- 21.1.3.55 and above

The correction is **already included** in the **release kits** of following versions:

- Fabasoft Folio / eGov-Suite 2022 Update Rollup 1 (22.0.1.x) and higher Update Rollup versions
- Fabasoft eGov-Suite 2022 April Release (from 22.4.0.x) and higher Feature Track versions
- Fabasoft Folio (22.5.0.x) and higher versions

3.3.3.3 Workaround: Disable Fabasoft Folio Client Update Service

The affected part of the Fabasoft Folio Client is the Fabasoft Folio Client Update Service, that is installed during the Fabasoft Folio Client installation.

This service is listed under Windows Services as

- "Fabasoft Folio Client 2022 Update Service", service name is "folioupdatepm22".
- "Fabasoft Folio Client 2021 Update Service", service name is "folioupdatepm21".

Set the service startup type to "Disabled" via Group Policy. By disabling these services, the security vulnerability cannot be exploited.

3.4 Spring Framework RCE via Data Binding on JDK 9+ Vulnerability (CVE-2022-22965)

First published 4 April 2022

Last update: 4 April 2022

ID: FSC33127

Affected Components: Identity Provider of the Fabasoft Cloud, Fabasoft Secomo

Severity: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H, Base Score: 9.8

Status: Final

CVE: CVE-2022-22965

3.4.1 Summary

A Spring MVC or Spring WebFlux application running on JDK 9+ may be vulnerable to remote code execution (RCE) via data binding. Two components of the Fabasoft Cloud used the Spring framework with the affected version: Identity Provider of the Fabasoft Cloud and Fabasoft Secomo.

3.4.2 Impact

Remote code execution (RCE) would have be potentially possible on the affected components.

3.4.3 Remediation

Fabasoft has provided a hotfix in the Fabasoft Cloud for all affected components on 01. April 2022 by updating the Spring framework to the latest version 5.3.18. No other remediation is required by the customer.

Note: Fabasoft Folio and the Fabasoft eGov-Suite do not make use of the Spring framework and are therefore not affected.

3.4.4 More Information

https://spring.io/blog/2022/03/31/spring-framework-rce-early-announcement

https://tanzu.vmware.com/security/cve-2022-22965

3.5 Risk to assign system admin privileges by restricted admin users (eGov14136)

First published: 10 March 2022

Last update: 11 March 2022

ID: eGov14136

Affected Components: Fabasoft eGov-Suite 2019/2020/2021/2022

Severity: not scored

Status: Final

CVEs: -

3.5.1 Summary

Users with a position that has not granted system administrative permissions, may have permissions to edit their own user object, allowing them to self-assign a user role / position with system administrative permissions.

In the Fabasoft eGov-Suite, some positions (like "Fachadministrator", "Mandantenadministrator" or "Dienststellenadministrator") are limited administrative positions, but have permissions to edit their own user object to add the "Systemadministration" position to their own and others user object.

Dependent to the Fabasoft Solution and custom ACLs at the customer's installation, the security leak may or may not be exploited by restricted administrators.

3.5.2 Impact

A Fabasoft eGov-Suite user with restricted administrative permissions (like "Fachadministrator", "Mandantenadministrator" or "Dienststellenadministrator") may be possible to edit the own user object. The user would be possible to add a user role with full administrative privileges.

3.5.3 Remediation

Please double-check all active user objects for the assigned user roles. Check, that only allowed users have the System Administration position.

3.5.3.1 Hotfix information

Fabasoft provides hotfixes for the following Fabasoft eGov-Suite versions:

- Fabasoft eGov-Suite 2022 (from 22.0.0.244.18)
- Fabasoft eGov-Suite 2021 Update Rollup 3 (from 21.1.3.24.121)
- Fabasoft eGov-Suite 2020 Update Rollup 5 (from 20.1.5.70.34)
- Fabasoft eGov-Suite 2019 Update Rollup 3 (from 19.2.3.131.51)

The correction is already included in:

- Fabasoft eGov-Suite 2022 Update Rollup 1
- Fabasoft eGov-Suite 2022 April Release

With the corrected functionality, a special security check is performed when the user roles and tenants are tried to be changed. Furthermore, an auditlog entry is written on any change of the user roles.

Fabasoft recommends to contact your Fabasoft representative to check your installation against the issue.

4 Vulnerabilities 2021

4.1 Apache Log4j Security Vulnerability (CVE-2021-44228, CVE-2021-45046, CVE-2021-45105)

First published: 13 December 2021

Last update: 22 December 2021

ID: FSC31322

Affected Components: Fabasoft Cloud, Fabasoft Folio

Severity: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H, Basic Score: 10.0 (Critical)

Status: Final

CVEs: CVE-2021-44228

Informations for another Log4j issues CVE-2021-45046 and CVE-2021-45105 see at the end of this article.

4.1.1 Information

A flaw was found in the Java logging library Apache Log4j in versions from 2.0.0 (including beta versions) up to and including 2.14.1. This allows a remote attacker to execute code on the server if the system logs an attacker-controlled string value with the attacker's JNDI LDAP server lookup.

In order to exploit this flaw you need:

- A remotely accessible endpoint with any protocol (HTTP, TCP, etc) that allows an attacker to send arbitrary data.
- A log statement in the endpoint that logs the attacker controlled data.

A lot of software products and libraries use the Log4j library and therefore may be affected.

4.1.1.1 Fabasoft Products

The following Fabasoft products may be affected by the vulnerability:

- Fabasoft Business Process Cloud
- Fabasoft Folio/eGov-Suite 2021 April Release (21.4.x)
- Fabasoft Folio/eGov-Suite 2021 July Release (21.7.x)
- Fabasoft Folio/eGov-Suite 2021 November Release (21.11.x)

Not affected:

- Fabasoft Folio/eGov-Suite 2021 Release, Update Rollup 1 and Update Rollup 2
- Fabasoft Folio/eGov-Suite 2022
- All versions below Fabasoft Folio/eGov-Suite 2021
- Fabasoft Mindbreeze Enterprise (all versions)
- Fabasoft app.telemetry (all versions)

Fabasoft Folio Client and Fabasoft Cloud Client are not affected in any version of Fabasoft Folio / Fabasoft eGov-Suite.

4.1.1.2 Double-Check for usage

You can check for the used library by doing a file search on your Fabasoft Folio and Mindbreeze servers:

Search for log4j* in:

Windows Folio: C:\Program Files\Fabasoft\

Windows Folio: C:\ProgramData\Fabasoft\INSTALLDIR

Windows Mindbreeze Enterprise: Search the full server for log4j*

Linux Folio: /var/opt/fabasoft/cache/INSTALLDIR

Linux Mindbreeze Enterprise: Search the full server for log4j*

4.1.1.3 Developing own solutions

If your company is developing own solutions or apps for your Fabasoft Folio installation with Java, check your repository for any Log4j dependencies. Also check all other used Java libraries that they haven't packaged the impacted Log4j library.

4.1.2 Solution in the Fabasoft Business Process Cloud

A hotfix was applied in the Fabasoft Business Process Cloud at 13. December 2021.

Mitigation measures were applied before. So far, there is no indication that the vulnerability has been exploited.

Although not affected, a version using log4j version 2.16.0 was applied in the Fabasoft Business Process Cloud at 19. December 2021.

Although not affected, a version using log4j version 2.17.0 was applied in the Fabasoft Business Process Cloud at 21. December 2021.

4.1.3 Hotfix information for Fabasoft Folio and Fabasoft eGov-Suite

Currently, a hotfix is available for:

Fabasoft Folio 2021 November Release (build 21.11.0.150)

Fabasoft eGov-Suite 2021 November Release (build 21.11.0.150.007)

Please contact Fabasoft Enterprise Support to request a hotfix package for this version. The hotfixed products use at least log4j version 2.17.0.

4.1.4 Mitigation for Fabasoft Folio

It is strongly recommended to install the provided hotfix for Fabasoft Folio 2021 November Release or Fabasoft eGov-Suite 2021 November Release.

With a Java option for Log4j, the LDAP lookup, that causes the vulnerability, may be disabled.

For affected Fabasoft Folio 2021 versions, please use this workaround to disable the vulnerability on all servers:

4.1.4.1 Windows

- Locate the file C:\ProgramData\Fabasoft
- Open the file coomk.upd
- If no entry HKEY_ENVIRONMENT\COOJAVA_JVMOPTIONS= is present, add HKEY_ENVIRONMENT\COOJAVA_JVMOPTIONS=-Dlog4j2.formatMsgNoLookups=true
- If the entry HKEY_ENVIRONMENT\COOJAVA_JVMOPTIONS= already exists with other parameters, add HKEY_ENVIRONMENT\COOJAVA_JVMOPTIONS=<someotherparameter> -

Dlog4j2.formatMsgNoLookups=true
(using a blank so seperate the entries)

Restart all Kernel instances on that machine.

4.1.4.2 Linux

Fabasoft Folio environment variables can be configured in two ways, see https://help.folio.fabasoft.com/index.php?topic=doc/Fabasoft-Folio-Envir... details.

Option 1 - Per server configuration

- Navigate to /etc/fabasoft/settings/users/fscsrv/Software/Fabasoft/Environment
- If not existing, create a directory COOJAVA_JVMOPTIONS or change to this directory.
- Create or edit a file named registry.default
- Add the following into the file
  -Dlog4j2.formatMsgNoLookups=true
- Make sure that no line-break is on the end of the file.
- Restart all Kernel instances on that machine.

Option 2 - Per service configuration

Also if using option 1, double-check that the server-wide setting is not overwritten by the per-service configuration.

- Repeat these steps for each <instance>:
- Navigate /var/opt/fabasoft/instances/ <instance> /env
- Check or create for a file named COOJAVA_JVMOPTIONS

Add the following into the file
-Dlog4j2.formatMsgNoLookups=true

Make sure that no line-break is on the end of the file.

Restart all Kernel instances on that machine.

4.1.5 Log4j 2.15.0. Vulnerability CVE-2021-45046 and Log4j 2.16.0 Vulnerability CVE-2021-45105

Additional vulnerabilities have been reported by the Log4j project (CVE-2021-45046 and CVE-2021-45105) when the logging configuration uses a non-default pattern layout.

Fabasoft Folio does not use the specific pattern layout in its code, therefore no Fabasoft Folio version and the Fabasoft Business Process Cloud are or were affected.

Nevertheless Fabasoft will update the Log4j library to version 2.17.0 to close CVE-2021-45105 in the hotfixed versions for CVE-2021-44228, and for all future releases.

Fabasoft Mindbreeze Enterprise does not use any of the vulnerable features, therefore no Fabasoft Mindbreeze Enterprise version is affected .

4.1.6 Log4j 1.2 Vulnerability CVE-2021-4104

During investigations another vulnerability for Log4j Version 1.2 was identified, that is listed under CVE-2021-4104 with CVSS v3 Base Score 8.1 (High).

No Fabasoft Folio version is affected by CVE-2021-4104.

4.2 Reflected Cross Site Scripting at First Request (FSC29337)

First published: 28 August 2021

Last update: 16 September 2021

ID: FSC29337

Affected Components: Fabasoft Folio Webservices, Fabasoft Cloud Webservices

Severity: CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N, Basic Score: 7.3

Status: Final

CVEs: -

4.2.1 Summary

By passing a malicious content in a parameter to the first request in the Fabasoft Folio web client, an error will be returned that reflects this content. The content type of the response is not interpreted correctly and the malicious content is injected on the web browser client.

4.2.2 Impact

An attacker may send a link to a user containing the malicious content. If the user opens the link in the web browser, code may be executed in the current usersâ€™ context.

4.2.3 Remediation

The parameter values are not part of the error message anymore.

4.2.3.1 Fabasoft Cloud

A hotfix was applied in the Fabasoft Cloud at 16. August 2021.

4.2.3.2 Fabasoft Folio / Fabasoft eGov-Suite

A hotfix is provided for all supported Fabasoft Folio / Fabasoft eGov-Suite versions. It is recommended to install this hotfix.

4.2.3.3 Hotfix Information (Fabasoft Folio)

Fixed with following versions of Fabasoft Folio:

- Fabasoft Folio Version 2021 Update Rollup 2 (21.1.2)

A hotfix is provided for the following Fabasoft Folio versions:

- Fabasoft Folio Version 2021 July Release (21.7.0)
- Fabasoft Folio Version 2021 Update Rollup 1 (21.1.1)
- Fabasoft Folio Version 2020 Update Rollup 5 (20.1.5)
- Fabasoft Folio Version 2020 Update Rollup 4 (20.1.4)
- Fabasoft Folio Version 2019 Update Rollup 3 (19.2.3)
- Fabasoft Folio Version 2017 R1 Update Rollup 7 (17.4.7)
- Fabasoft Folio Version 2017 R1 Update Rollup 6 (17.4.6)
- and all major releases and Update Rollups above the mentioned versions.

4.2.3.4 Hotfix Information (Fabasoft eGov-Suite)

Fixed with following versions of Fabasoft eGov-Suite:

- Fabasoft eGov-Suite 2021 Update Rollup 2 (21.1.2)

A hotfix is provided for the following Fabasoft eGov-Suite versions:

- Fabasoft eGov-Suite 2021 July Release (21.7.0)
- Fabasoft eGov-Suite 2021 Update Rollup 1 (21.1.1)
- Fabasoft eGov-Suite 2020 Update Rollup 5 (20.1.5)
- Fabasoft eGov-Suite 2020 Update Rollup 4 (20.1.4)
- Fabasoft eGov-Suite 2019 Update Rollup 3 (19.2.3)

5 Vulnerabilities 2020

5.1 Folio Client Mailmerge interruption can lead to wrong content (FSC25088)

First published: 23 November 2020

Last update: 12 February 2021

ID: FSC25088

Affected Components: Fabasoft Folio Client with Fabasoft eGov-Suite

Severity: CVSS:3.1/AV:L/AC:L/PR:H/UI:R/S:U/C:H/I:N/A:N, Basic Score: 4,2 (Medium)

Status: New

CVEs: -

5.1.1 Summary

Running the mail-merge process from within Fabasoft eGov-Suite (that is processed by the locally installed Folio Client), and the user opens other Word documents during mail-merge processing, the wrong content could be applied as mail-merge result.

5.1.2 Impact

In the case that the user opens a Word document beneath the mail-merge process, the Folio Client wrongly assumes that the opened document is the result of the mail-merge. The document with wrong content is assigned to the receipient of the mail-merge, and in consequence may be sent to a receipient of the mail-merge.

The wrongly used content may include personally identifiable or confidential information.

5.1.3 Remediation

Fabasoft has fixed the issue. A hotfix is available for Fabasoft Folio versions listed in the hotfix section.

The fix requires to update the Fabasoft Folio Client on the client machines. No update of other services is required.

5.1.3.1 Workaround

As long as the Fabasoft Folio Client was not updated to the build numbers mentioned below, recommend your users to not open any other Microsoft Word documents as long as the progress bar of the mail-merge is visible.

5.1.3.2 Hotfix Information

Fabasoft has fixed this issue in the following Fabasoft Folio / Fabasoft eGov-Suite versions:

- Fabasoft Folio 2021 (from Folio Client version 21.1.0.76)
- Fabasoft Folio 2020 Update Rollup 4 (from Folio Client version 20.1.4.50)
- Fabasoft Folio 2019 Update Rollup 3 (from Folio Client version 19.2.3.175)
- Fabasoft Folio 2017 R1 (from Kit 17.4.0.73 / from Folio Client version 17.4.7.114)
- Fabasoft Folio 2017 R1 UR7 (from Folio Client version 17.4.7.114)
- Fabasoft Folio 2016 Update Rollup 7 (from Kit 16.0.11.77 / from Folio Client version 16.0.11.77)
- and all major releases and Update Rollups above the mentioned versions.

5.2 Access to Confidential Data Possible via Image Conversion (FSC21814)

First published: 14 May 2020

Last update: 25 November 2020

ID: FSC21814

Affected Components: Fabasoft Cloud Web Services, Fabasoft Folio Web Services

Severity: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N, Basic Score: 6,5 (Medium)

Status: Final

CVEs: CVE-2018-16323

5.2.1 Summary

Due to the vulnerability CVE-2018-16323 in ImageMagick when converting images and downloading them memory fragments can be leaked via the image data

5.2.2 Impact

By repeated downloading converted images an attacker can read parts of the memory of a Fabasoft Web Service that may contain sensitive information.

5.2.3 Remediation

5.2.3.1 Hotfix Information

Fixed with following versions of the Fabasoft Cloud or Fabasoft Folio:

- Fabasoft Cloud Version 2020 June Release (Version 20.3.1)
- Fabasoft Folio Version 2021 (Version 21.1.0)

5.3 Malicious Website can Perform Actions Through Fabasoft Cloud or Fabasoft Folio Browser Extension (FSC21815)

First published: 14 May 2020

Last update: 25 November 2020

ID: FSC21815

Affected Components: Fabasoft Cloud Client, Fabasoft Folio Client

Severity: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:L, Basic Score: 8.3 (High)

Status: Final

CVEs: -

5.3.1 Summary

The Fabasoft Cloud or Fabasoft Folio browser extension uses web messaging to communicate with the Fabasoft Cloud Client or Fabasoft Folio Client. The Fabasoft Cloud Client or Fabasoft Folio Client do not check whether the origin of the messages is a trustworthy site.

5.3.2 Impact

Malicious website can perform actions through Fabasoft Cloud or Fabasoft Folio browser extension and store files in the temp directory of the current user.

5.3.3 Remediation

5.3.3.1 Fabasoft Cloud

If you do not have the auto-update enabled, update the Fabasoft Cloud Client to its current version. No further action is required for the Fabasoft Cloud Client.

5.3.3.2 Fabasoft Folio

Update the Fabasoft Folio Client to the version mentioned below. Moreover, it is strongly recommended to restrict the communication with the Fabasoft Folio Client to particular hosts or domains. This can be done by setting an appropriate registry key.

For more information concerning this setting of the Fabasoft Folio Client refer to topic „Security Considerations of the Fabasoft Folio Client Web Browser Integration" in the Whitepaper „Fabasoft Folio Client" (https://help.folio.fabasoft.com/index.php?topic=doc/Fabasoft-Folio-Clien...)

5.3.3.3 Hotfix Information

Fixed with following versions of the Fabasoft Cloud or Fabasoft Folio Client:

- Fabasoft Cloud Version 2020 June Release (Version 20.3.1)
- Fabasoft Folio Client Version 2020 UR 2 (Version 20.1.2)
- Hotfix for Fabasoft Folio Client Version 2019 UR3
- Hotfix for Fabasoft Folio Client Version 2017 R1 UR6

6 Vulnerabilities earlier than 2020

6.1 glibc vulnerability (CVE-2015-7547)

First published: 19 February 2016

Last update: 25 November 2020

ID: -

Affected Components: Red Hat Enterprise Linux / CentOS

Severity: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H, Basic Score: 8.1 (High)

Status: Final

CVEs: CVE-2015-7547

6.1.1 Information

The following information was made available by Red Hat concerning this vulnerability: A stack-based buffer overflow was found in the way the libresolv library performed dual A/AAAA DNS queries. A remote attacker could create a specially crafted DNS response which could cause libresolv to crash or, potentially, execute code with the permissions of the user running the library. Note: this issue is only exposed when libresolv is called from the nss_dns NSS service module.

For further information, please refer to the References section.

6.1.2 Solution

At the moment we do not know about specific security issues in our products based on this vulnerability.

Regardless of this, we advise that all Linux servers using a vulnerable version of glibc are patched immediately, as there might be currently unknown situations or other vulnerable services active that may compromise the systems integrity.

Following an update of glibc there may be a change in the locale settings leading to a different localisation appearance for some Fabasoft products (eg. timestamps, currency display).
If you experience problems, such as an incorrect date format, please rerun the setup of the Fabasoft product to correct the system settings. For further information, please refer to the Applies to section.

Reruninng the Setup is required for versions earlier than

- Fabasoft eGov-Suite 2013
- Fabasoft Folio 2012 Spring Release

6.1.3 References

- CVE-2015-7547 (Red Hat)
- CVE-2015-7547 (Mirte)
- CVE-2015-7547: glibc getaddrinfo stack-based buffer overflow

6.1.3.1 Applies to

- Fabasoft Folio
- Fabasoft eGov-Suite
- Fabasoft Mindbreeze

6.2 glibc "GHOST" vulnerability (CVE-2015-0235)

Last update: 6 November 2020

6.2.1 Summary

This is an advisory regarding a security issue in the glibc library also known as GHOST.

6.2.2 Information

The following information was made available by Red Hat concerning this vulnerability: A heap-based buffer overflow was found in glibc's __nss_hostname_digits_dots() function, which is used by the gethostbyname() and gethostbyname2() glibc function calls. A remote attacker able to make an application call either of these functions could use this flaw to execute arbitrary code with the permissions of the user running the application.

For further information, please refer to the References section.

6.2.3 Solution

Current analysis of our products indicated that there is no known security issue based on this vulnerability.

Regardless of this, we advise that all Linux servers using a vulnerable version of glibc are patched immediately, as there might be currently unknown situations or other vulnerable services active that may compromise the systems integrity.

Following an update of glibc there may be a change in localisation for some Fabasoft products. If you experience problems, such as an incorrect date format, please rerun the setup of the Fabasoft product to correct the system settings

6.2.4 References

- RHSA-2015:0092-1 - Critical: glibc security update (Red Hat)
- CVE-2015-0235 (Mirte)
- Critical glibc update (CVE-2015-0235) in gethostbyname() calls
- Ghost: Uralte LÃ¼cke in Glibc bedroht Linux-Server (Heise)

6.2.4.1 Applies to

- Fabasoft Folio
- Fabasoft eGov-Suite
- Fabasoft Mindbreeze

6.3 Bash vulnerability (CVE-2014-6271 and CVE-2014-7169)

Last update: 6 November 2020

6.3.1 Summary

This is an information regarding a security issue in the Unix Bash (Bourne Again Shell) commonly used in Linux environments as well as Mac OS.

6.3.2 Information

CVE-2014-6271
A flaw was found in the way Bash evaluated certain specially crafted environment variables. An attacker could use this flaw to override or bypass environment restrictions to execute shell commands. Certain services and applications allow remote unauthenticated attackers to provide environment variables, allowing them to exploit this issue.

CVE-2014-7169
This CVE describes the incomplete fix of CVE-2014-6271 in the first round of patches

For further information, please refer to the References section.

6.3.2.1 Fabasoft Products

Due to the fact that Fabasoft products do not use CGI Scripts on Linux environments they are not directly affected by this vulnerability.

6.3.3 Solution

We strongly suggest you immediately install the latest patches for the bash executable on all systems!

All major Linux distribution have released patches, both for the original and the followup CVE. So far there are no known problems with either of these patches. As of writing this article the second patch has not yet been distributed to all patch mirrors, due to this it is advised to verify the version of the patch provided from your mirror.

6.3.4 References

- NVD - Vulnerability Summary for CVE-2014-6271
- NVD - Vulnerability Summary for CVE-2014-7169
- CVE - CVE-2014-6271
- CVE - CVE-2014-7169
- Update on CVE-2014-6271: Vulnerability in bash (shellshock)

6.3.4.1 Applies to

- All Fabasoft products running on an Linux environment

6.4 ImageMagick vulnerability (CVE-2016-3714, CVE-2016-3718, FSC03839)

First published: 09 May 2016

Last update: 25 November 2020

ID: FSC03839

Affected Components: Fabasoft Folio

Severity: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H, Basic Score: 8.4 (High)

Status: Final

CVEs: CVE-2016-3714 , CVE-2016-3718

6.4.1 Information

There are multiple vulnerabilities in ImageMagick, a package commonly used by web services to process images. One of the vulnerabilities can lead to remote code execution (RCE) if you process user submitted images. The exploit for this vulnerability is being used in the wild.

For further information, please refer to the References section.

6.4.1.1 Solution

Currently it is possible to deactivate the vulnerable conversions by including the following lines in the <policymap> tag of your policy.xml for ImageMagick:

```
<policy domain="coder" rights="none" pattern="EPHEMERAL" />
<policy domain="coder" rights="none" pattern="URL" />
<policy domain="coder" rights="none" pattern="HTTPS" />
<policy domain="coder" rights="none" pattern="MVG" />
<policy domain="coder" rights="none" pattern="MSL" />
<policy domain="coder" rights="none" pattern="TEXT" />
<policy domain="coder" rights="none" pattern="SHOW" />
<policy domain="coder" rights="none" pattern="WIN" />
<policy domain="coder" rights="none" pattern="PLT" />
```

Please be aware that adding the above lines will currently lead to an error while converting svg files.

6.4.2 How to apply

6.4.2.1 Linux

- Add the above mentioned lines to the /etc/fabasoft/magick/policy.xml file.
- Restart the Fabasoft Folio web and conversion services in order to ensure that all processes take the new configuration into consideration (**a reload is not sufficient**).

6.4.2.2 Windows

- Create a new environment variable named MAGICK_CONFIGURE_PATH and point it to a directory which all service users are allowed to access.
- Download the standard policy.xml from the ImageMagick website and save it to this directory (*https://www.imagemagick.org/source/policy.xml*).
- Edit the file and add the lines mentioned above.
- Restart the Fabasoft Folio web and conversion services in order to ensure that all processes take the new configuration into consideration (**a reload is not sufficient**).

6.4.2.3 Hotfix information

The fixed ImageMagick library is shipped with Fabasoft Folio from these versions:

- Fabasoft Folio 2013 UR6 (from 13.0.13.36)
- Fabasoft Folio 2014 UR6 (from 14.0.13.42)
- Fabasoft Folio 2015 UR3 and above
- Fabasoft Folio 2016 UR1 and above
- Fabasoft Folio 2017
- and all higher Fabasoft Folio versions and Update Rollups

6.4.3 References

- CVE - CVE-2016-3714
- CVE - CVE-2016-3715
- CVE - CVE-2016-3716
- CVE - CVE-2016-3717
- CVE - CVE-2016-3718
- ImageTragick
- ImageMagick: Resources listing

6.4.3.1 Applies to

- All current versions

6.5 http.sys MS15-034 vulnerability (CVE-2015-1635)

First published: 15 April 2015

Last update: 25 November 2020

ID:

Affected Components: Fabasoft Folio on Microsoft Windows Server 2008 R2, Microsoft Windows Server 2012 and R2

Severity: AV:N/AC:L/Au:N/C:C/I:C/A:C, Basic Score: 10.0 (High)

Status: Final

CVEs: CVE-2015-1635

6.5.1 Summary

This is an information regarding a security issue in the Windwos HTTP protocol stack (HTTP.sys) used in Windows Operating Systems. Most importantly this vulnerability affects the Internet Information System (IIS) Component of Windwos Server environments.

6.5.2 Information

CVE-2015-1635
HTTP.sys in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8, Windows 8.1, and Windows Server 2012 Gold and R2 allows remote attackers to execute arbitrary code via crafted HTTP requests, aka "HTTP.sys Remote Code Execution Vulnerability."

Fabasoft Products
Our internal tests when using the KB3042553 provided by Microsoft have shown no negative effects on any of our products

6.5.3 Solution

We strongly recommend you to install the Microsoft KB3042553 Patch on all systems!

So far there are no known problems with this patch.

6.5.4 References

- Microsoft Security Bulletin MS15-034 - Critical
- CVE-2015-1635
- NVD - Vulnerability Summary for CVE-2015-1635

6.5.4.1 Applies to

All Fabasoft products running on Windows 7, Windows Server 2008 R2, Windows 8, Windows Server 2012, Windows 8.1, and Windows Server 2012 R2

6.6 Java vulnerability (CVE-2014-4244)

Last update: 6 November 2020

6.6.1 Summary

This is an information regarding a security issue in Oracle Java SE (Standard Edition) and Oracle JRockit.

6.6.2 Information

An undisclosed vulnerability has been found in Oracle Java SE (Standard Edition) and Oracle JRockit.

According to the Oracle Critical Patch Update Advisory - July 2014 this vulnerability applies to "...client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service."

For further information, please refer to the References section.

6.6.3 Solution

6.6.3.1 Oracle Java SE 6 Update 75 and lower

Although the CVE-2014-4244 vulnerability also applies to versions of Java SE 6 Update 75 (6u75) and earlier, the support for Java SE 6 has expired and new versions of Java SE 6 are only available through the Java SE Support program. Therefore, assistance with the upgrade of Java SE 6 can only be provided by your Oracle software vendor.

6.6.3.2 Oracle Java SE 7 Update 60 and lower

If you are using Java SE 7 Update 60 (7u60) or lower we recommend to update to Java SE 7 Update 65 (7u65), available from Oracle.

The Java binary is used in a wide range of Fabasoft products, including Fabasoft Folio, Fabasoft eGov-Suite and Fabasoft Mindbreeze.

Warning: Upgrading your Java SE version may lead to unexpected behaviour. Please test extensively before issuing the update on a productive system.

6.6.3.3 Fabasoft Folio / Fabasoft eGov-Suite

For all versions of Fabasoft Folio and Fabasoft eGov-Suite that support Java SE 7, no additional steps need to be taken after upgrading the Java SE version.

6.6.3.4 Fabasoft Mindbreeze

If you are using a version of Fabasoft Mindbreeze that supports Java SE 7, you need to apply a hotfix in addition to updating to Java SE 7 Update 65.

Note: If you require the aforementioned hotfix for your Fabasoft Mindbreeze installation, please contact Fabasoft Support.

6.6.3.5 Oracle Java SE 8 Update 5 and lower

Currently no versions of Fabasoft products require Java SE 8 in any affected version.

6.6.4 References

- CVE-2014-4244

- NVD - Vulnerability Summary for CVE-2014-4244
- Oracle Critical Patch Update Advisory - July 2014

6.6.4.1 Applies to

- Fabasoft Folio
- Fabasoft eGov-Suite
- Fabasoft Mindbreeze

6.7 OpenSSL "Heartbleed" vulnerability (CVE-2014-0160)

Last update: 6 November 2020

6.7.1 Summary

This is an information regarding a security issue in the OpenSSL library.

Notice: This is an urgency released article. Further information may be added, therefore please re-check for information updates.

6.7.2 Information

A severe programming error has been identified in the OpenSSL library, which affects the most recent versions of the OpenSSL library. A missing bounds check in the handling of the TLS heartbeat extension can be used to reveal up to 64k of memory to a connected client or server.

More information can be found at:

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160
- http://heartbleed.com/
- http://www.heise.de/security/meldung/Der-GAU-fuer-Verschluesselung-im-Web-Horror-Bug-in-OpenSSL-2165517.html (German)

6.7.3 Solution

If you use SSL on your server for any service we strongly suggest that you make sure your server is not vulnerable, and if it is vulnerable that you apply the fixes which have already been provided by most operating system vendors.

The OpenSSL library is used in a wide range of Fabasoft products as well, including Fabasoft Folio, Fabasoft eGov-Suite, Fabasoft Mindbreeze and Fabasoft app.telemetry.

6.7.3.1 Fabasoft Folio / Fabasoft eGov-Suite

The **IMAP Server** functionality in the following Fabasoft Folio versions may be affected (both Microsoft Windows and Linux):

- Fabasoft Folio 2012 Fall Release
- Fabasoft Folio 2013 Winter Release (fixed with Update Rollup 1 for Fabasoft Folio 2013 Winter Release)
- Fabasoft eGov-Suite 2013 (fixed with Update Rollup 1 for Fabasoft eGov-Suite 2013)
- Fabasoft Folio 2013 Spring Release
- Fabasoft Folio 2013 Summer Release
- Fabasoft Folio 2013 Fall Release

- Fabasoft Folio 2014 Winter Release (fixed with Update Rollup 1 for Fabasoft Folio 2014 Winter Release)
- Fabasoft Folio 2014 Spring Release

If you use Fabasoft IMAP Server in one of these listed versions, please contact Fabasoft Support to request a hotfix with an updated OpenSSL library.

Also other parts of Fabasoft Folio / Fabasoft eGov-Suite are using OpenSSL statically or included in a Fabasoft binary, but only for internal service communication, not for communication between users and Fabasoft Folio / Fabasoft eGov-Suite. Therefore the risk of the OpenSSL security issue is much lower in this area. Hotfixes with an updated OpenSSL library are available as listed above.

6.7.3.2 Fabasoft products potentially affected by a vulnerable operating system's OpenSSL library

Fabasoft products and components installed on Linux operating systems are using the OpenSSL library of the operating system:

- Fabasoft Folio and eGov-Suite Services running on Apache webserver with SSL (Web services, Conversion services, and so on)
- Mindbreeze Enterprise Search Client Services and Management
- Fabasoft app.telemetry Server
- Fabasoft app.telemetry Agent

Fabasoft suggests to update all affected operating systems to the latest OpenSSL library. Fabasoft products installed under Microsoft Windows use the unaffected Microsoft SSL implementation.

6.7.3.3 Applies to

- Fabasoft Folio 2012 Fall Release
- Fabasoft Folio 2013 Winter Release
- Fabasoft eGov-Suite 2013
- Fabasoft Folio 2013 Spring Release
- Fabasoft Folio 2013 Summer Release
- Fabasoft Folio 2013 Fall Release
- Fabasoft Folio 2014 Winter Release
- Fabasoft Folio 2014 Spring Release

6.8 Liferay Portlet Cross-Site Scripting vulnerability

First published: 6 November 2013

Last update: 6 November 2013

ID: -

- Affected Components: Fabasoft Folio (up to and including 2012 Fall Release), Fabasoft eGov-Suite (up to and including 2012)

Severity: (not measured)

Status: Final

CVEs: (unknown)

6.8.1 Summary

A security vulnerability was found in the Fabasoft Portlet for Liferay that can allow Cross Site Scripting, if an attacker modifies the URL in a special way.

6.8.2 Information

An attacker can exploit this vulnerability to run JavaScript code on the client machine.

An article about the risks of cross-site scripting (XSS) can be found at Wikipedia.

Webservers and services in the backend are not affected by this vulnerability. No code execution can be done on these machines. Only client machines are at risk.

6.8.3 Solution

A hotfix for the portlet is available for the Fabasoft software versions listed below.

If you use a Liferay production environment in an insecure network (Internet), please open a ticket at Fabasoft Service Desk including your current Fabasoft Folio/eGov-Suite version.

6.8.4 Applies to

- Fabasoft Folio (up to and including 2012 Fall Release)
- Fabasoft eGov-Suite (up to and including 2012)
- Hotfix-Builds with build number 12.0.7.116 and above already include the hotfix

6.9 MHTML Script Injection vulnerability (Microsoft KB 2501696)

6.9.1 Information

On January 28th 2011 Microsoft has released the Security Advisory 2501696 concerning a MHTML Script Injection vulnerability in Microsoft Internet Explorer. In context of this Security Advisory and respectively KB 2501696 Microsoft released a FixIt to address this issue preliminary to an official hotfix. According to Microsoft the only side effects they have encountered are script execution and ActiveX being disabled within MHT documents.

As Microsoft expects limited impacts in most environments due to the changes mentioned above, exploratory tests have shown no impact on Fabasoft Folio or the Fabasoft eGov-Suite. These tests have been performed using

- Fabasoft Folio 2010 Fall Release
- Fabasoft Folio 2010 Summer Release
- Fabasoft Folio 2010 Spring Release
- Fabasoft Folio 2009 Fall Release
- Fabasoft eGov-Suite 8.0 SP1
- Fabasoft eGov-Suite 8.0
- Fabasoft eGov-Suite 7.0 SP3
- Fabasoft eGov-Suite 7.0 SP2

In general, Fabasoft Folio 2009 Fall Release (and higher) respectively Fabasoft eGov-Suite 8.0 (and higher) might not be affected as MHT is not used (e.g. for object-overviews) in these versions. As PDF-overviews are used instead we can't see an impact on these versions.

In contrast Fabasoft eGov-Suite 7.0 SP2 and SP3 used MHT e.g for file overviews and could be affected by this security enhancement by Microsoft. Nevertheless, no impact could be found in our basic tests using file-overviews and file-documentations.

Please note that no comprehensive regression testing has been performed. This information is provided "as is" with no warranties. We suggest further testing in your environment if you are planning to deploy this security enhancement.

7 Security Vulnerabilities Mindbreeze Enterprise / Mindbreeze InSpire

Known Security Vulnerabilities of Mindbreeze InSpire and Mindbreeze Enterprise Search are listed on Mindbreeze's website:

https://inspire.mindbreeze.com/support/vulnerabilities