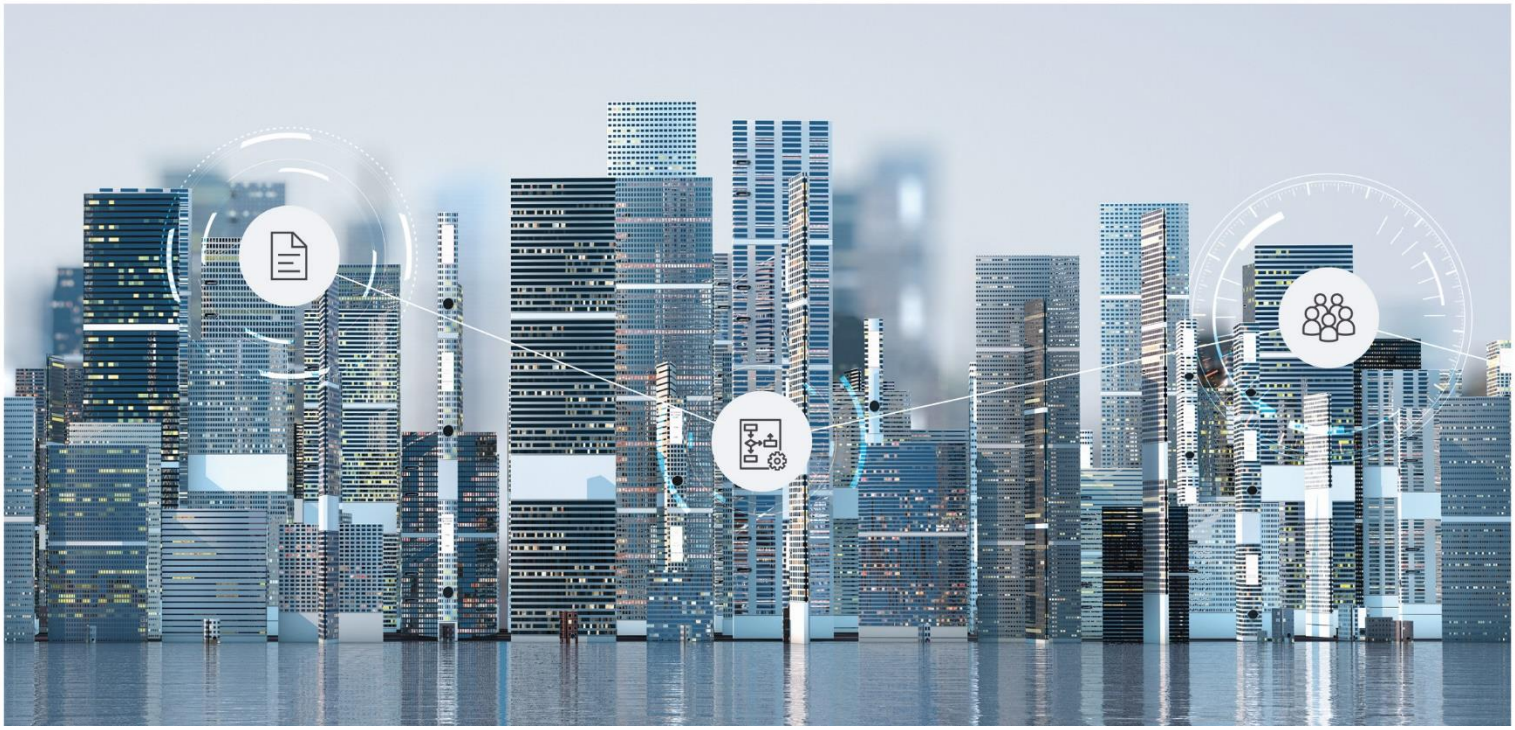
Fabasoft



Security Vulnerabilities

Fabasoft Business Process Cloud

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 2022

1.1 Text4Shell CVE-2022-42889 information

First published: 21 October 2022

Last update: 27 October 2022

ID: PDO03176

1.1.1 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.

1.1.2 Impact

No Fabasoft products are impacted by the Text4Shell vulnerability.

1.1.3 Remediation

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

1.1.3.1 Fabasoft Business Process Cloud

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

1.1.3.2 Fabasoft Folio / Fabasoft eGov-Suite

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

1.1.4 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.

1.2 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: -

1.2.1 Summary

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

1.2.2 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.

1.2.3 Remediation

The cross site scripting vulnerability is fixed.

1.2.3.1 Fabasoft Cloud

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

1.2.3.2 Fabasoft Folio

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

1.2.4 Hotfix Information

Fixed with following versions Fabasoft Folio:

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

1.3 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: -

1.3.1 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.

1.3.2 Impact

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

1.3.3 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.

1.3.3.1 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.

1.3.3.2 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

1.3.3.3 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.

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

First published 04 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

1.4.1 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.

1.4.2 Impact

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

1.4.3 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.

1.4.4 More Information

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

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

2 Vulnerabilities 2021

2.1 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.

2.1.1 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.

2.1.1.1 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.

2.1.1.2 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*

2.1.1.3 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.

2.1.2 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.

2.1.3 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.

2.1.4 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:

2.1.4.1 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.

2.1.4.2 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.

2.1.5 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** .

2.1.6 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.

2.2 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: -

2.2.1 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.

2.2.2 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.

2.2.3 Remediation

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

2.2.3.1 Fabasoft Cloud

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

2.2.3.2 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.

2.2.3.3 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.

2.2.3.4 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)

3 Vulnerabilities 2020

3.1 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

3.1.1 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

3.1.2 Impact

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

3.1.3 Remediation

3.1.3.1 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)

3.2 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: -

3.2.1 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.

3.2.2 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.

3.2.3 Remediation

3.2.3.1 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.

3.2.3.2 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...)

3.2.3.3 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