

```

m sul
Tar
Bw
1.1
Mu
Vol

git u=|
tar
bw
1-
17-
5-

git sta
tar
bw
1-
17-
5-

git url
tar
bw
1-
17-
5-

```

Tangro BWF 1.17.5 ist anfällig für mehrere Sicherheitslücken, die unter anderem durch eine fehlerhafte Zugriffskontrolle und unsichere direkte Objektreferenzierung (IDOR) ausgelöst werden:

- ## Detailed Security Advisories

<p><b>Product:</b> Tangro BWF</p> <p><b>Vendor:</b> tangro software components GmbH (Heidelberg, Germany)</p> <p><b>Tested Version:</b> 1.17.5</p> <p><b>Fixed Version:</b> 1.18.1</p> <p><b>Vulnerability Type:</b> Insecure Direct Object Reference</p> <p><b>CVSSv2 Severity:</b> AV:N/AC:L/Au:S/C:N/I:P/A:N (Score 4.0)</p> <p><b>CVSSv3 Severity:</b> AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N (Score 4.3)</p> <p><b>CWE Reference:</b> CWE-639</p> <p><b>CVE Reference:</b> CVE-2020-26171</p> <p><b>Authors:</b> Dimitri Lesy &amp; Tobias Györfi, Thinking Objects GmbH</p>	
<p><b>### Overview</b></p> <p>The "documentId" of attachment uploads to "/api/document/attachments/upload" can be manipulated. By doing this, users can add attachments to work.</p> <p><b>### Proof of Concept</b></p>	

<p><b>Product:</b> Tangro BWF</p> <p><b>Vendor:</b> tangro software components GmbH (Heidelberg, Germany)</p> <p><b>Tested Version:</b> 1.17.5</p> <p><b>Fixed Version:</b> 1.18.1</p> <p><b>Vulnerability Type:</b> Session Fixation</p> <p><b>CVSSv2 Severity:</b> AV:N/AC:H/Au:N/C:P/I:P/A:N (Score 4.0)</p> <p><b>CVSSv3 Severity:</b> AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N (Score 4.2)</p> <p><b>CWE Reference:</b> CWE-294</p> <p><b>CVE Reference:</b> CVE-2020-26172</p> <p><b>Authors:</b> Dimitri Lesy &amp; Tobias Györfi, Thinking Objects GmbH</p> <p><b>### Overview</b></p> <p>Every login in Tangro generates the same JWT token, which allows an attacker to reuse the token when a session is active. The JWT token does not</p> <p><b>### Proof of Concept</b></p>	
--	--

## Unauthenticated PDF Download (CVE-2020-26173)

**Product:** Tangro BWF  
**Vendor:** tangro software components GmbH (Heidelberg, Germany)  
**Tested Version:** 1.17.5  
**Fixed Version:** 1.18.1  
**Vulnerability Type:** Incorrect Access Control  
**CVSSv2 Severity:** AV:N/AC:H/Au:N/C:P/I:N/A:N (Score 2.6)  
**CVSSv3 Severity:** AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N (Score 3.1)  
**CWE Reference:** CWE-639  
**CVE Reference:** CVE-2020-26173  
**Authors:** Dimitri Lesy & Tobias Györfi, Thinking Objects GmbH

### ### Overview

PDF files of invoices are served over the "/api/pdf/<documentID>" API endpoint and secured using an additional token:

`https://<Tangro Hosts>/api/pdf/00000000000000123456?token=<Token>`

## Upload Filetype Constraint Bypass (CVE-2020-26174)

**Product:** Tangro BWF  
**Vendor:** tangro software components GmbH (Heidelberg, Germany)  
**Tested Version:** 1.17.5  
**Fixed Version:** 1.18.1  
**Vulnerability Type:** Upload Filetype Constraint Bypass  
**CVSSv2 Severity:** AV:N/AC:L/Au:S/C:C/I:C/A:C (Score 9.0)  
**CVSSv3 Severity:** AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H (Score 8.8)  
**CWE Reference:** CWE-434  
**CVE Reference:** CVE-2020-26174  
**Authors:** Dimitri Lesy & Tobias Györfi, Thinking Objects GmbH

### ### Overview

The Tangro application requests a list of allowed filetypes from the server and restricts uploads to the filetypes contained in this list. However,

### ### Proof of Concept

## Profile Attributes of Other Users Writable (CVE-2020-26175)

**Product:** Tangro BWF  
**Vendor:** tangro software components GmbH (Heidelberg, Germany)  
**Tested Version:** 1.17.5  
**Fixed Version:** 1.18.1  
**Vulnerability Type:** Insecure Direct Object Reference  
**CVSSv2 Severity:** AV:N/AC:L/Au:S/C:N/I:C/A:N (Score 6.8)  
**CVSSv3 Severity:** AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N (Score 6.5)  
**CWE Reference:** CWE-639  
**CVE Reference:** CVE-2020-26175  
**Authors:** Dimitri Lesy & Tobias Györfi, Thinking Objects GmbH

### ### Overview

The value of "PERSON" in requests to /api/profile can be manipulated in order to change profile information of other users.

### ### Proof of Concept

...  
POST /api/profile HTTP/1.1  
Host: <Tangro Host>

## Unauthorised Listing of Attachments (CVE-2020-26176)

**Product:** Tangro BWF  
**Vendor:** tangro software components GmbH (Heidelberg, Germany)  
**Tested Version:** 1.17.5  
**Fixed Version:** 1.18.1  
**Vulnerability Type:** Insecure Direct Object Reference  
**CVSSv2 Severity:** AV:N/AC:L/Au:S/C:P/I:N/A:N (Score 4.0)  
**CVSSv3 Severity:** AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N (Score 4.3)  
**CWE Reference:** CWE-639  
**CVE Reference:** CVE-2020-26176  
**Authors:** Dimitri Lesy & Tobias Györfi, Thinking Objects GmbH

### ### Overview

No or broken access control checks exist on the "/api/document/<DocumentID>/attachments" API endpoint.

Knowing a document ID, it is possible to list all the attachments of a workitem, including their respective IDs. This allows an attacker to gather

## Editing Disabled Profile Attributes (CVE-2020-26177)

**Product:** Tangro BWF  
**Vendor:** tangro software components GmbH (Heidelberg, Germany)  
**Tested Version:** 1.17.5  
**Fixed Version:** 1.18.1  
**Vulnerability Type:** Incorrect Access Control  
**CVSSv2 Severity:** AV:N/AC:L/Au:S/C:N/I:P/A:N (Score 4.0)  
**CVSSv3 Severity:** AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N (Score 4.3)  
**CWE Reference:** CWE-639  
**CVE Reference:** CVE-2020-26177  
**Authors:** Dimitri Lesy & Tobias Györfi, Thinking Objects GmbH

### ### Overview

A user's profile contains some items that are greyed out and thus are not intended to be edited by regular users. However, this restriction is on Manipulating any of the greyed out values in requests to "/api/profile" is not prohibited server-side.

### ### Remediation

## Unauthenticated Download of Workitem Attachments (CVE-2020-26178)

**Product:** Tangro BWF  
**Vendor:** tangro software components GmbH (Heidelberg, Germany)  
**Tested Version:** 1.17.5  
**Fixed Version:** 1.18.1  
**Vulnerability Type:** Insecure Direct Object Reference  
**CVSSv2 Severity:** AV:N/AC:L/Au:N/C:P/I:N/A:N (Score 5.0)  
**CVSSv3 Severity:** AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N (Score 5.3)  
**CWE Reference:** CWE-639  
**CVE Reference:** CVE-2020-26178  
**Authors:** Dimitri Lesy & Tobias Györfi, Thinking Objects GmbH

### ### Overview

Knowing an attachment ID, it is possible to download workitem attachments without being authenticated.

### ### Proof of Concept

<https://<Tangro Host>/api/document/attachment/<AttachmentID>?archiveName=D1&fileType=/SSC/PDF>

### ### Remediation

## Disclosure Timeline

2020-09-17: Vulnerability discovered  
2020-10-01: Vulnerability reported to vendor  
2020-10-01: Vendor responded immediately  
2020-10-21: Vulnerability fix implemented, software update enters QA  
2020-11-04: Vulnerability fixed, software update 1.18.1 released  
2020-12-17: Vulnerability disclosed

## References

[1] Advisory URL: <https://blog.to.com/advisory-tangro-bwf-1-17-5-multiple-vulnerabilities> (<https://blog.to.com/advisory-tangro-bwf-1-17-5-multiple-vulnerabilities>)

[2] Tangro Website: <https://www.tangro.de/> (<https://www.tangro.de/>)

## Disclaimer

The information provided in this security advisory is provided „as is“ and without warranty of any kind. Details of this security advisory may be updated in order to provide as accurate information as possible. The latest version of this security advisory is available on <https://blog.to.com>.

Copyright: [Creative Commons – Attribution \(by\) – Version 3.0](https://creativecommons.org/licenses/by/3.0/deed.en) (<http://creativecommons.org/licenses/by/3.0/deed.en>).

Autor/in



**Tobias  
Györfi**

(<https://blog.to.com/author/tobias-gyoerfi/>)

IT-Security Consultant

## Top Blogbeiträge



**Wissen Sie, was auf ihrer Firewall vor sich geht?**(<https://blog.to.com/firewall-carewoche-regelwerk-review/>)



**Corona-Warn-App – Welche Daten werden geteilt?**(<https://blog.to.com/corona-warn-app-daten/>)



**Vulnerability Scan – Grenzen und Chancen**(<https://blog.to.com/vulnerability-scan-pt-2/>)

## Dies könnte Sie auch interessieren



**Wie wird man Penetrationstester?**

(<https://blog.to.com/penetrationstester/>)

Bei einem Penetrationstest (oft Pentest genannt) testen Penetrationstester, auch Ethical Hackers genannt, die Sicherheit eines IT-Systems. Dabei kann es sich z. B. um ein Computernetzwerk, eine Website oder eine Smartphone-App handeln. Ziel ist das frühzeitige Identifizieren von Schwachstellen in dem System, um es danach gegen Angreifer schützen zu können.



**Advisory: ActFax 7.10 Build 0335 Privilege Escalation (CVE-2020-15843)**

(<https://blog.to.com/advisory-actfax-7-10-build-0335-privilege-escalation-cve-2020-15843/>)

Während eines Penetrationstests ist mir aufgefallen, dass ActFax 7.10 Build 0335 in der Standardkonfiguration eine Sicherheitslücke enthält. Nach der Installation verfügt die Benutzergruppe „Everyone“ über die vollständige Kontrolle des „Terminal“ Verzeichnisses. Hierdurch kann jeder angemeldeter Benutzer alle Dateien des Verzeichnisses manipulieren. Diese Berechtigungskonfiguration kann zu einer Privilege Escalation führen.



**Advisory: SuperWebMailer < 7.40.0.01550 Unauthenticated Remote Code Execution (CVE-2020-11546)**

(<https://blog.to.com/advisory-superwebmailer-cve-2020-11546/>)

Die Versionen vor 7.40.0.01550 des SuperWebMailer sind anfällig für eine Remote Code Execution Sicherheitslücke (RCE). Die Anwendung verarbeitet die Language-Variable ohne ausreichende Sicherheitsprüfung und reicht diese intern in ein eval(), was einem unauthentifzierten Angreifer die Ausführung von beliebigem PHP Code im Kontext des Webservers erlaubt (CWE-94). Die Sicherheitslücke ist laut Hersteller in Version 7.40.0.01550 behoben worden (8.4.2020).

Advisory    CVE    IDOR    Tangro BWF

## Schreibe einen Kommentar

Deine E-Mail-Adresse wird nicht veröffentlicht. Erforderliche Felder sind mit \* markiert.

## KOMMENTAR

NAME \*

E-MAIL \*

WEBSITE



MEINEN NAMEN, E-MAIL UND WEBSITE IN DIESEM BROWSER SPEICHERN, BIS ICH WIEDER KOMMENTIERE.

CAPTCHA \*

ACHT – = 2 ↺

Kommentar abschicken



(<https://www.xing.com/companies/thinkingobjectsgmbh>)



(<https://de.linkedin.com/company/thinking-objects-gmbh>)



(<https://twitter.com/thinkingobjects>)



(<https://www.youtube.com/channel/UCvkXLivj61AEbZs3Wh49L5w>)



(<https://www.facebook.com/TopalisGruppe>)

